



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Provvedimento del 25 settembre 2025 [10185463]

[doc. web n. 10185463]

Provvedimento del 25 settembre 2025

Registro dei provvedimenti
n. 531 del 25 settembre 2025

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il cons. Angelo Fanizza, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (di seguito, "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione n. 98 del 4 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. 1098801;

RELATORE l'avv. Guido Scorza;

PREMESSO

1. Introduzione.

L'Autorità ha appreso da notizie di stampa della stipula di un protocollo d'intesa tra la Provincia Autonoma di Bolzano - Alto Adige (di seguito, la "Provincia"), Comuni, Commissariato del Governo, Questura e Forze dell'Ordine, avente ad oggetto l'installazione sul territorio della Provincia di una rete di centoventiquattro telecamere, dotate di funzionalità di lettura

automatizzata delle targhe dei veicoli in transito, sia per l'analisi dei flussi di traffico, volta a orientare le politiche in materia di mobilità e infrastrutture, sia per la prevenzione e l'accertamento di reati.

2. L'attività istruttoria.

Nel corso dell'istruttoria avviata sulla base delle predette notizie di stampa, l'Autorità ha rivolto alla Provincia alcune richieste d'informazioni (v. note prot. nn. XX del XX; XX del XX; n. XX del XX; XX del XX), la Provincia, nel fornire riscontro alle stesse (v. note prot. nn. XX del XX; XX del XX; XX del XX), ha dichiarato, in particolare, che:

“[...] il progetto [...] rientra nelle finalità istituzionali dell'Amministrazione provinciale così come previsto dagli art. 13 comma 7 e 227 del “Nuovo Codice della Strada”, dal Decreto del Presidente della Repubblica 22 marzo 1974 n. 381 [...] nonché dalla Deliberazione della Giunta Provinciale n. 683 del 06/08/2019 [...]”;

“il progetto [consiste nella] rilevazione dei flussi di traffico in Alto Adige tramite lettura delle targhe [...]”;

“[...] le [...] telecamere poste lungo la rete stradale effettuano la lettura delle targhe degli autoveicoli e non salvano le foto [...]”;

“[i] dati statistici ed aggregati vengono utilizzati per pianificare una serie di misure relativamente al traffico, anche in un'ottica di salvaguardia ambientale ed economica dell'area Dolomiti-UNESCO e delle successive aree sensibili che sono state via via aggiunte al progetto”;

“le telecamere sono state installate ed attivate [come segue]: da XX (24 telecamere); da XX (7 telecamere); da XX (8 telecamere); da XX (60 telecamere); da XX (12 telecamere); da XX (13 telecamere)”.

“l'informativa di secondo livello è stata resa disponibile agli interessati presso gli Uffici tecnici della Ripartizione Servizio strade della Provincia Autonoma di Bolzano a far tempo dal XX”;

“[...] è stata quindi effettuata una revisione del testo, che ha dato luogo a una seconda versione aggiornata, in data XX, messa a disposizione presso gli stessi Uffici”;

“tale versione è stata altresì messa a disposizione in data XX sia presso gli uffici, sia online al link <https://www.provincia.bz.it/turismo-mobilita/strade/manutenzione/monitoraggio-del-traffico.asp>, sul sito web istituzionale del Servizio strade della Provincia Autonoma di Bolzano”;

“gli attuali cartelli contenenti l'informativa di primo livello sono stati installati tra il XX ed il primo XX, in sostituzione dei precedenti cartelli [...]”;

“[...] gli interventi della Provincia devono essere motivati e devono garantire che siano evitate applicazioni discriminatorie o irragionevoli, il che impone, necessariamente, la raccolta di dati il più possibile oggettivi e puntuali sui flussi di traffico, dunque, e necessariamente, una prodromica fase di monitoraggio degli stessi, non potendosi motivare una scelta se non muovendo da dati oggettivi”;

“l'attività in questione è espressamente contemplata in una norma di rango primario [...], ovvero] l'art. 19 del D.P.R. 22 marzo 1974, n. 381 [...]”;

“i numeri delle targhe e gli altri dati metadati associati a ciascuna di esse [...] non vengono

mai [...] a conoscenza della Provincia [...] le videocamere sono protette da password nota esclusivamente al responsabile del trattamento (società [fornitrice]) e non al titolare (Provincia) [...]”;

“la Provincia [...] ha accesso [...] unicamente [al]l’insieme finale di numeri progressivi associati a flussi di origine e destinazione del traffico”;

“l’intero processo [...] si svolge integralmente all’interno del “guscio” tecnologico del responsabile del trattamento, rispetto al quale esiste una perfetta segregazione da parte della Provincia”;

“[...] deve escludersi che la targa costituisca, nella vicenda in esame, un dato personale [...], poiché la stessa non] è incrociata con la banca dati [dell’] Automobile Club d’Italia [...] il responsabile del trattamento non è autorizzato a [...] procedere a fare match di qualsiasi tipo tra i dati processati e altre informazioni”;

“[...] tali numeri [di targa] costituiscono [in ogni caso] dati anonimi per l’Amministrazione e dati pseudonimizzati per il responsabile del trattamento [...]”;

la Provincia “non dispone [infatti] di alcuna chiave di decifratura”.

“l’elaborazione in forma aggregata è [...] realizzata associando set di dati a una stringa di hash, e non più a un numero di targa”;

- “[...] il sistema è stato configurato in maniera tale da creare report fino a 2 anni [...] per] permettere [...] di disporre di dati concreti per la programmazione di interventi sulla rete stradale che permettano di gestire e ottimizzare efficacemente [...] i flussi di traffico [...]”;
- “i dispositivi video sono collocati anche nel territorio della Provincia Autonoma di Trento [di seguito, la “Provincia di Trento”], in virtù della [stipula di una] convenzione”;
- “la Proprietà civilistica delle prime 24 videocamere, quelle cioè oggetto della menzionata convenzione, è di entrambe le Province”;
- la Provincia di Trento ha approvato la predetta convenzione con il verbale di deliberazione della Giunta Provinciale reg. delib. n. 1192 del 12 agosto 2019;
- “la convenzione [...] è l’unico accordo” stipulato tra le due Province;
- “[...] la collocazione delle videocamere; la scelta delle stesse; la scelta dei dati da acquisire attraverso esse; la scelta del fornitore [...] la logica da applicare ai dati al fine di ottenere le matrici O/D del traffico e la determinazione della tipologia dello stesso (turistico, di attraversamento, residenziale, pendolare) sono state determinate dalla Provincia Autonoma di Bolzano”;
- “la Provincia [...] di Trento è intervenuta solo sul piano economico, non dispone [...] di alcun contatto diretto con [l’Azienda], ma ha diritto di chiedere direttamente alla Provincia Autonoma di Bolzano dati di output aggregati”.

Alla luce delle dichiarazioni rese dalla Provincia, l’Autorità ha coinvolto nell’istruttoria l’azienda fornitrice della soluzione tecnologica (di seguito, l’“Azienda”), in veste di responsabile del trattamento, rivolgendo alla stessa una richiesta d’informazioni (v. nota prot. n. XX del XX). L’Azienda, con nota del XX, ha dichiarato, in particolare, che:

- “[...] il set di dati raccolti dalle telecamere [è il seguente:] l’identificatore della telecamera (codice assegnato alla singola telecamera), data, ora, minuto, secondo del passaggio del mezzo sotto la telecamera, la classe del mezzo, la sua nazionalità (se presente), eventuali codici KEMLER (merci pericolose) nonché, se presente, la velocità di transito”;
- “la [...] Azienda non esegue interrogazioni al Pubblico Registro Automobilistico (P.R.A.) [...], non essendo] l’attività svolta non è in alcun modo diretta all’identificazione di persone fisiche”;
- “la targa in chiaro viene eliminata entro al massimo 60 secondi dal ricevimento. Da essa viene creata una prima stringa hash salted (primo livello di protezione), la quale viene a sua volta eliminata entro 60 secondi dalla conversione dopo la creazione di una seconda stringa hash salted (secondo livello di protezione)”;
- “entrambe le funzioni di hash, descritte precedentemente utilizzano la funzione SHA256. I valori di salt utilizzati non variano nel tempo. In base ad un algoritmo ed a seconda del codice alfanumerico della targa, viene utilizzato uno degli oltre 200 differenti salt presenti nel sistema. Solo il subtitolare del trattamento, unica persona in grado di accedere alle banche dati, è a conoscenza dell’algoritmo e degli oltre 200 differenti salt utilizzati prima delle due funzioni di crittazione hash. L’algoritmo è unidirezionale e funzione della targa in arrivo. Già dopo l’applicazione del primo salt e funzione SHA256 sulla targa sarà impossibile, anche per il subtitolare del trattamento, risalire dal codice hash (protezione di primo livello) alla targa. Ciò nonostante, viene applicato un secondo salt e funzione SHA256, ottenendo un ulteriore nuovo codice hash (protezione di secondo livello). Solo tale ultimo codice hash verrà salvato all’interno della banca dati. La targa in arrivo e il codice hash (protezione di primo livello) non vengono memorizzate”.

Con nota del XX (prot. n. XX), l’Ufficio, sulla base degli elementi acquisiti, dalle verifiche compiute e dei fatti emersi a seguito dell’attività istruttoria, ha notificato alla Provincia, ai sensi dell’art. 166, comma 5, del Codice, l’avvio del procedimento per l’adozione dei provvedimenti di cui all’art. 58, par. 2, del Regolamento, per aver la Provincia posto in essere un trattamento di dati personali in violazione degli artt. 5, par. 1, lett. a) ed e), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 12, par. 1, 13, 21, par. 4, 26 e 35 del Regolamento, nonché 2-ter del Codice. Con la medesima nota, il predetto titolare è stato invitato a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall’Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, della l. 24 novembre 1981, n. 689).

Con nota dell’XX (prot. n. XX), la Provincia ha presentato una memoria difensiva, esponendo gli argomenti difensivi in dettaglio illustrati e presi in considerazione nel successivo par. 3. La Provincia non si è avvalsa del diritto di chiedere di essere audita dall’Autorità ai sensi dell’art. 166, comma 6, del Codice.

3. Esito dell’attività istruttoria.

3.1. Sull’asserita inosservanza dei termini procedurali.

In sede di memoria difensiva, la Provincia ha eccepito che sussisterebbe “ampia inosservanza di termini perentori”, non avendo l’Autorità osservato il “termine di 120 giorni dall’accertamento della violazione”, di cui alla “Tabella B, punto 2) del Reg. GPDP n. 2/2019 per la notificazione”, tenuto conto che “procedimento è durato oltre 16 mesi. Nello specifico: in data XX l’Autorità ha dato avvio al procedimento amministrativo nei confronti della Provincia con la formulazione di alcuni quesiti; il successivo XX la Provincia ha fornito riscontro; il XX seguiva ulteriore richiesta del Garante; il XX

perveniva riscontro della Provincia; l'XX spirava, quindi, il termine suddetto di 120 giorni; il successivo XX, e addirittura dopo 123 giorni dall'ultimo riscontro (facendo cioè in ipotesi decorrere un nuovo termine di 120 giorni dal XX), il Garante inviava nuova richiesta di chiarimenti; il XX, in un'ottica di cortesia e piena collaborazione con l'Autorità, la Provincia, forniva comunque puntuale riscontro; decorrevano a questo punto addirittura 282 giorni da tale ultimo riscontro e oltre 400 giorni (sospensioni incluse) dal termine iniziale del XX, quando il XX, l'Autorità trasmetteva alla Provincia l'ennesima richiesta di chiarimenti su questioni che avrebbe dovuto affrontare entro l'XX";

Al riguardo, occorre formulare alcune precisazioni in ordine ai termini procedurali applicabili alla notificazione alla Provincia delle contestate violazioni, come previsti dal Regolamento del Garante n. 2/2019.

Premesso che al procedimento amministrativo in oggetto non si applica il termine di 90 giorni di cui alla l. del 24 novembre 1981, n. 689 ma quello pari a 120 giorni specificatamente individuato, ai sensi dell'art. 154, comma 3 e dell'art. 166, comma 9 del Codice, con il predetto Regolamento del Garante n. 2/2019, si evidenzia che detto termine decorre "dall'accertamento della violazione" (v. Tabella B, parte 2) del Regolamento del Garante n. 2/2019) e che la data dell'accertamento è da individuarsi nel momento in cui tanto la raccolta degli elementi istruttori quanto la valutazione dei medesimi da parte dell'amministrazione procedente siano state portate a compimento (v., in tal senso, Cass. dell'8 agosto 2005, n. 16642; v., anche, Cass. Sez. II civ. del 28 novembre 2012, n. 21114 e Cass. Sez. II civ. del 22 aprile 2016, n. 8204).

Per quanto in particolare concerne l'attività delle Autorità amministrative indipendenti, merita di essere segnalato che la Suprema Corte, nel solco di consolidati indirizzi giurisprudenziali, ha stabilito che l'attività di accertamento dell'illecito, in relazione alla quale collocare il dies a quo del termine per la notifica degli estremi della violazione, non può coincidere con il momento in cui viene acquisito il fatto nella sua materialità, ma deve essere intesa come comprensiva del tempo necessario alla valutazione dei dati acquisiti ed afferenti gli elementi (oggettivi e soggettivi) dell'infrazione e, quindi, della fase finale di deliberazione correlata alla complessità, nella fattispecie, delle indagini tese a riscontrare la sussistenza dell'infrazione medesima e ad acquisire piena conoscenza della condotta illecita, sì da valutarne la consistenza agli effetti della corretta formulazione della contestazione (cfr. Cass. nn. 13050/2014, 1043/2015, 770/2017, 31635/2018 e 21500/2024).

Analogamente, con specifico riferimento agli illeciti amministrativi di cui alla normativa in materia di protezione dei dati personali, la Suprema Corte ha poi recentemente ribadito che "la pura "constatazione" dei fatti non comporta di per sé il loro "accertamento", per gli effetti di cui all'art. 166 [del Codice], ove occorra una successiva attività istruttoria e valutativa ai fini dell'efficiente espletamento dell'attività sanzionatoria" (Cass. civ., sez. I, n. 18583/2025; v. già, ancorché in riferimento al termine di 90 giorni previsto dall'art. 14 della l. 689/1981, Cass. civ., sez. 2, n. 18288/2020).

Sul punto si fa, peraltro, presente che, come rilevato dalla giurisprudenza di legittimità, in caso di più violazioni connesse fra di loro, "la congruità del tempo complessivamente impiegato" dall'amministrazione procedente ai fini dell'accertamento delle predette violazioni è da intendersi come strettamente connessa "alla complessità dell'attività di indagine" posta in essere dalla medesima (v. Cass. Sez. I civ. del 4 aprile 2018, n. 8326).

Preme, inoltre, considerare che il suindicato termine di 120 giorni "è sospeso dal 1° al 31 agosto di ciascun anno e riprende a decorrere dalla fine del periodo di sospensione" (v. art. 6, comma 1 del Regolamento del Garante n. 2/2019).

Alla luce di quanto sopra chiarito in ordine ai termini procedurali applicabili al caso di specie, come

previsti dalla normativa vigente, deve ritenersi che la notificazione alla Provincia delle contestate violazioni, effettuata dall'Ufficio con nota del XX, non sia stata intempestiva, tanto più se si considera l'elevato grado di complessità della fattispecie oggetto del presente procedimento amministrativo, che ha richiesto accertamenti istruttori che hanno coinvolto non solo la Provincia ma anche l'Azienda fornitrice e la Provincia di Trento, acquisendo elementi istruttori imprescindibili ai fini della definizione del complessivo quadro istruttorio.

In ogni caso, quanto al rispetto del richiamato termine di 120 giorni, decorrente "dall'accertamento della violazione", ed entro il quale occorre effettuare la "comunicazione delle presunte violazioni (articolo 166, comma 5, del Codice)" (v. Tabella B, n. 2, del citato Regolamento del Garante n. 2/2019), deve osservarsi che - in disparte da ogni valutazione in merito all'effettiva perentorietà di tale termine alla luce della più recente giurisprudenza della Corte di giustizia dell'Unione europea (v. sent. C-510/23, *Trenitalia*, del 30 gennaio 2025) - nel caso di specie detto termine è stato comunque pienamente rispettato. Il riscontro della Provincia all'ultima delle richieste d'informazioni dell'Ufficio (v. nota del XX, prot. n. XX) è stato, infatti, acquisito al protocollo dell'Autorità del XX (n. XX) e, pertanto, la contestazione di violazione amministrativa del XX è stata notificata alla Provincia in un arco temporale di soli 25 giorni. Soltanto a fronte di tale ultimo riscontro, vertente, in particolare, sulla ricostruzione del ruolo soggettivo della Provincia e della Provincia di Trento nel contesto di trattamento in questione, si poteva, infatti, ritenere conclusa e definita la complessiva istruttoria avviata nei confronti della Provincia, con il conseguente "accertamento della violazione".

Quanto poi all'invocata giurisprudenza di merito, in base alla quale l'Autorità sarebbe tenuta al rispetto del predetto termine di 120 giorni anche ai fini dell'eventuale invio di multiple richieste d'informazioni ai soggetti coinvolti nel procedimento, volte a chiarire o integrare gli elementi istruttori già acquisiti, deve farsi presente - senza in questa sede fare rilievi in merito a tale orientamento giurisprudenziale - che, nel caso di specie, contrariamente a quanto sostenuto dalla Provincia in sede di memoria difensiva, tutte le richieste d'informazioni formulate nel corso dell'istruttoria hanno comunque rispettato tale tempistica asseritamente vincolante per l'autorità di controllo procedente. Infatti, alla prima richiesta d'informazioni del XX è stato fornito riscontro con nota del XX, acquisita al protocollo dell'Autorità nella medesima data; la seconda richiesta d'informazioni del XX è, dunque, stata proposta nell'arco temporale di 20 giorni da detto riscontro della Provincia; la terza richiesta d'informazioni è stata formulata in data XX, ovvero nell'arco temporale di 120 giorni dalla data in cui è stata acquisita al protocollo dell'Autorità - n. XX del XX - la nota del XX con cui la Provincia ha fornito riscontro alla seconda richiesta d'informazioni; la quarta richiesta d'informazioni è stata formulata nei confronti dell'Azienda, con la Provincia in copia per opportuna conoscenza, in data XX, ovvero nell'arco temporale di 118 giorni dalla data in cui è stata acquisita al protocollo dell'Autorità - n. XX del XX - la nota della medesima data con cui la Provincia ha fornito riscontro alla terza richiesta d'informazioni; la quinta richiesta d'informazioni è stata formulata nei confronti Provincia in data XX, ovvero, tenendo conto del periodo di sospensione feriale dal XX al XX, nell'arco temporale di 113 giorni dalla data in cui è stata acquisita al protocollo dell'Autorità - n. XX dell'XX - la nota del XX con cui l'Azienda ha fornito riscontro alla quarta richiesta d'informazioni. Ciò fermo restando che il momento dell'accertamento della violazione non può comunque coincidere formalisticamente con la data in cui un certo documento è stato acquisito agli atti dell'Autorità, essendo sempre necessaria un'attività di valutazione e approfondimento da parte dell'Ufficio, finalizzata all'effettivo "accertamento della violazione", tenendo in considerazione tutti gli elementi istruttori complessivamente acquisiti con le diverse richieste d'informazioni, specialmente nell'ambito di istruttorie complesse, anche sul piano tecnologico, e che coinvolgono a vario titolo diversi soggetti, come quella di cui trattasi.

3.2. Il trattamento di dati personali posto in essere dalla Provincia e la natura di dati personali delle informazioni raccolte.

Risulta accertato che la Provincia, a partire dal mese di XX, ha installato sul territorio interessato dal progetto n. 124 telecamere, dotate di funzionalità di lettura automatizzata delle targhe dei

veicoli in transito. In particolare, l'installazione di tali dispositivi video è stata effettuata con la seguente tempistica: da XX, n. 24 telecamere; da XX, ulteriori n. 7 telecamere; da XX, ulteriori n. 8 telecamere; da XX, ulteriori n. 60 telecamere; da XX, ulteriori n. 12 telecamere; da XX, ulteriori n. 13 telecamere. Tali dispositivi sono in grado di estrapolare informazioni in merito alla classe dei veicoli in transito (moto, auto, bus, furgone, mezzo pesante, altro), alla nazionalità, all'eventuale classe di velocità, all'eventuale codice KEMLER, nonché all'origine e destinazione del viaggio, consentendo di comprendere e analizzare i flussi di traffico all'interno dell'area Dolomiti-UNESCO e di adottare scelte amministrative coerenti con le effettive caratteristiche dei flussi di traffico in tale area.

I dati relativi alle targhe dei veicoli in transito sono raccolti inizialmente in chiaro e conservati per "massimo 60 secondi", per poi essere ulteriormente elaborati.

In relazione a tale prima fase del trattamento, deve osservarsi che i numeri di targa sono da considerarsi senza dubbio alcuni quali "dati personali" relativi a proprietari e agli utilizzatori dei veicoli ad essi associati, in quanto informazioni relative a persone fisiche identificabili (art. 4, par. 1, n. 1), del Regolamento), anche per effetto della possibilità per chiunque di consultare il pubblico registro automobilistico (PRA). Ciò trova, altresì, conferma nella giurisprudenza della Corte di Cassazione, che ha affermato che "è indubbio che l'informazione di cui si discute - la targa di un autoveicolo, in quanto riferita a soggetto identificato o identificabile - deve considerarsi "dato personale". Lo era giusta l'art. 4, lett. b), del d.lgs. n. 196/2003 [...] [e] lo è tuttora, ai sensi del Regolamento (UE) 2016/679" (Cass. civ., Sez. I, ord. del 18 dicembre 2023, n. 35256; v. anche Cass. civ., Sez. I, ord. del 7 luglio 2021, n.19270, ove si afferma che "particolarmente importanti sono i dati che permettono [...] l'identificazione indiretta, come un numero di identificazione (ad esempio, [...] il numero di targa)".

Non rileva, a tal riguardo, come sostenuto dalla Provincia in sede di memoria difensiva, che non vengano di fatto effettuate interrogazioni del PRA o che non vi sarebbe, da parte della Provincia o dell'Azienda, uno specifico interesse ad effettuare tali interrogazioni, non essendo il progetto finalizzato a identificare specifiche persone fisiche e ad avviare procedimenti amministrativi nei confronti delle stesse. La qualificazione di un'informazione relativa a una persona fisica quale dato personale e il riconoscimento all'interessato della tutela garantita dalla normativa europea in materia di protezione dei dati prescinde, infatti, dall'animus del titolare del trattamento e dalla sua effettiva volontà di acquisire o meno le informazioni ulteriori che sono necessarie ai fini dell'identificazione degli interessati, rilevando esclusivamente la sussistenza in astratto di "mezzi [...] di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare [una] persona fisica direttamente o indirettamente" (cons. 26 del Regolamento). Diversamente interpretando, infatti, gli interessati si troverebbero caso per caso provvisti o sprovvisti di tutela con riguardo al trattamento di propri dati personali sulla base di una circostanza, ovvero la mera intenzione, soltanto dichiarata dal titolare, di procedere o meno all'identificazione degli stessi, che non sarebbe oggettivamente verificabile. Inoltre, indipendentemente dalla volontà del titolare e come evidenziato nel richiamato cons. 26 del Regolamento, l'operazione di identificazione di una persona fisica può ben essere effettuata anche da terzi che vi abbiano interesse, tanto nel contesto di attività del tutto lecite (es. richieste di acquisizione dei dati da parte delle Forze dell'ordine o dell'Autorità giudiziaria nell'ambito di attività di polizia giudiziaria) o illecite (es. attacchi di criminali informatici), facendo ricorso ai mezzi ragionevolmente a loro disposizione per conseguire l'identificazione degli interessati, che, nel caso di specie, consistendo in pubblici registri, sono pacificamente utilizzabili.

Ciò chiarito, si osserva che dall'istruttoria è, altresì, emerso che il numero di targa di ciascun veicolo in transito viene convertito, previa applicazione di un salt (selezionato in modo deterministico, anche sulla base dello stesso numero di targa, tra gli oltre 200 differenti salt presenti nel sistema), in un primo valore di hash, calcolato mediante la funzione di hashing SHA-256. Al termine di tale conversione, che avviene entro 60 secondi dal transito, il numero di targa

viene cancellato. Il primo valore di hash, così ottenuto, viene a sua volta convertito, previa applicazione di un salt, in un secondo valore di hash, calcolato mediante la funzione di hashing SHA-256. Al termine di tale seconda elaborazione, che avviene entro ulteriori 60 secondi, il primo valore di hash viene cancellato. Al secondo valore di hash viene poi associato un numero progressivo. L'associazione tra il secondo valore di hash e il numero progressivo, che costituiscono entrambi degli identificativi univoci del veicolo, viene memorizzata all'interno di un primo database; i dati relativi al transito del veicolo (numero progressivo, velocità ed eventuale codice KEMLER del veicolo, data e ora del transito, identificativo del dispositivo video) vengono, invece, memorizzati all'interno di un secondo database e conservati per due anni.

Contrariamente a quanto sostenuto dalla Provincia nel corso dell'istruttoria, tali operazioni conseguono unicamente la pseudonimizzazione delle informazioni relative ai veicoli in transito, essendo comunque possibile risalire agli stessi, non venendo, pertanto, meno la loro natura di dati personali. La pseudonimizzazione costituisce, infatti, una misura che può essere adottata per garantire la minimizzazione dei dati, la selettività degli accessi alle informazioni, in ossequio al principio di privacy by design e by default, nonché un livello di sicurezza adeguato al rischio, che non fa però venir meno la natura di dato personale delle informazioni a essa sottoposte (v. art. 32, par. 1, lett. a), del Regolamento). Il cons. 26 del Regolamento chiarisce, infatti, che "i dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile" (cfr., ex multis, le "Linee guida 1/2022 sui diritti degli interessati - Diritto di accesso", adottate dal Comitato europeo per la protezione dei dati il XX, ove si evidenzia che "i dati personali sottoposti a pseudonimizzazione sono ancora dati personali, al contrario dei dati anonimizzati"; v. anche il "Parere 1/2017 relativo alla proposta di regolamento sulla vita privata e le comunicazioni elettroniche (2002/58/CE)" del 4 aprile 2017 - WP 247, con il quale il Gruppo di lavoro Art. 29 - ora Comitato europeo per la protezione dei dati -, ancorché con riferimento ai c.d. Mac Address e in un diverso contesto, ha chiarito che gli "indirizzi MAC sono dati personali e lo restano anche dopo l'adozione di misure di sicurezza quali l'hashing").

La stessa Corte di giustizia dell'Unione europea ha affermato che "dall'articolo 4, punto 5, del RGPD, in combinato disposto con tale considerando 26 di tale regolamento, risulta che i dati personali che sono stati soltanto oggetto di pseudonimizzazione e che potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di informazioni supplementari devono essere considerati informazioni su una persona fisica identificabile, ai quali si applicano i principi relativi alla protezione dei dati" (Causa C-683/21, Nacionalinis visuomens sveikatos centras, del 5 dicembre 2023, par. 57 e 58).

Né rileva che l'intero processo di pseudonimizzazione, mediante funzioni di hash, sia posto in essere non già direttamente dalla Provincia ma da un proprio fornitore, che agisce, in ogni caso, per suo conto in qualità di responsabile del trattamento, ancorché la Provincia non disponga direttamente delle informazioni aggiuntive necessarie ad attribuire i dati a specifici interessati (proprietari/conducenti dei veicoli), venendo a conoscenza esclusivamente di dati su base aggregata. Occorre, infatti, evidenziare che sul titolare del trattamento, in quanto soggetto sul quale ricadono le decisioni circa le finalità e le modalità del trattamento dei dati personali degli interessati, grava una "responsabilità generale" sui trattamenti posti in essere (v. cons. 74 del Regolamento; cfr., tra i tanti, provv. 1° dicembre 2022, n. 409, doc. web n. 9833530 e i precedenti provv. ivi richiamati; v. anche le "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del [Regolamento]", adottate dal Comitato europeo per la protezione dei dati il 7 luglio 2021, spec. par. 174). Pertanto, "tale titolare del trattamento può vedersi infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83 del [Regolamento] in una situazione in cui i dati personali sono oggetto di un trattamento illecito e non è siffatto titolare del trattamento, bensì un responsabile del trattamento, di cui esso si è avvalso, che ha effettuato tale trattamento per conto del titolare", essendo irrilevante che "tale ente non ha

proceduto, esso stesso, a operazioni di trattamento di tali dati”; pertanto, dall’articolo 4, punto 7, del RGPD [...], lett[o] alla luce del considerando 74 del RGPD, risulta, [...] che un ente, qualora soddisfi la condizione posta da detto articolo 4, punto 7, è titolare non solo di qualsiasi trattamento di dati personali che esso stesso effettua, ma anche di quello effettuato per suo conto” (Corte di giustizia dell’Unione europea, sent. C-683/21, Nacionalinis visuomens sveikatos centras, del 5 dicembre 2023).

Altrettanto irrilevante è la circostanza che il trattamento dei dati personali in chiaro, prima dell’applicazione della funzione di hash, avvenga entro una limitata frazione temporale di circa sessanta secondi. La durata del trattamento è, infatti, influente ai fini della valutazione della liceità dello stesso e, anche quando il trattamento abbia una durata estremamente ridotta, il titolare non è esonerato dall’obbligo di assicurarsi che sussista un’idonea base giuridica che possa giustificare lo stesso (v., da ultimo, provv.ti 11 gennaio 2024, n. 5, doc. web n. 9977020, e 13 aprile 2023, nn. 122 e 123, doc. web n. 9896412 e doc. web n. 9896808).

Al riguardo, nell’ambito della propria memoria difensiva, la Provincia ha sostenuto che:

“l’“hash” [...] ha precise caratteristiche matematiche, tra le quali quella dell’irreversibilità. È cioè una funzione one-way, nessuno, neppure [l’Azienda], e neppure volendo, è in grado di invertirla, e ciò per oggettiva impossibilità matematica”;

“non potendo invertirla, anche ove [l’Azienda] conservasse le targhe d’origine, anziché cancellarle immediatamente (come invece fa), non sarebbe comunque assolutamente in grado di individuare, partendo da una stringa di hash, una precisa targa tra quelle (in ipotesi) conservate. Presa cioè una stringa di hash, dovrebbe ricalcolare daccapo tutti gli hash delle targhe in ipotesi conservate fino a trovare quello identico a quello cercato, e tenere traccia via via del processo (cioè creare una tabella di associazione)”;

“ma [l’Azienda], by design, non conserva né le targhe né tiene traccia del processo di generazione di ogni singolo hash da una data targa. Solo se conservasse targhe e traccia del processo [...], l’hash in questione sarebbe uno pseudonimo nel senso dell’art. 4.5) [del Regolamento], disposizione che postula infatti la conservazione separata delle “informazioni aggiuntive”. In mancanza di conservazione dei dati originari e di una tabella che li associ agli hash, questi ultimi non sono, nei termini del Regolamento, degli “pseudonimi”, a ciò difettando la definizione dell’art. 4.5)”;

“[...] tali ulteriori informazioni conservate [dall’Azienda] assolutamente non vi sono, né risultano ad esito dell’istruttoria, ed è evidente che non si può portare in consultazione al PRA un hash, per di più salted, ma solo una targa”;

“accade cioè che [l’Azienda]: non conservi assolutamente alcuna tabella di associazione tra ogni targa e ogni hash; non conservi neppure le targhe originarie, ma le cancelli non appena avvenuta la conversione in hash; non disponga cioè né di due database da incrociare (database delle targhe e database degli hash) e neppure di una tabella di associazione; conservi unicamente gli hash. In definitiva, perciò, [l’Azienda] non è in grado, a partire dai soli hash, di ricostruire a ritroso le targhe originarie e quindi di consultare il P.R.A.”;

“[...] il processo di salting, addirittura nella specie un doppio processo, permette di escludere anche l’ipotesi di scuola di attacchi da parte di terzi che entrassero abusivamente in possesso degli hash, perché i dati sarebbero completamente inutilizzabili per essi, punto che dimostra peraltro la qualità delle misure di sicurezza adottate”;

“ai fini della nozione di “dato personale” occorrono due precise condizioni giuridiche cumulative: 1. identificabilità concreta dell’interessato, ai sensi del considerando 26 [del

Regolamento]; 2. qualificabilità del dato come informazione su una persona fisica. [...] Nella specie, nessuna di queste due condizioni sussiste: non abbiamo cioè né soggetti concretamente identificabili né informazioni che li riguardino”;

“non si può interrogare il P.R.A. inviando un hash. Occorre risalire alla targa, ma, trattandosi di funzione one-way, ciò non è matematicamente possibile. Dato un certo hash non è possibile individuare la targa, ciò che fa venire meno “il significativo rischio per gli interessati”. È possibile solo creare l’hash dalla targa, non il contrario”;

“ciò significa che [l’Azienda], se volesse esporre a rischio gli interessati, dovrebbe: 1. creare ex novo un immenso database di tutte le targhe italiane e straniere circolanti; 2. conservarlo (anziché cancellare le targhe decorsi 60 secondi); 3. ricalcolare a partire da tale database delle targhe un nuovo database di hash, creando di volta in volta (e salvando) una tabella di associazione targa-hash durante tale processo [...]; 4. confrontare questo secondo database di hash con il primo e, tramite la tabella di associazione, collegare i valori del primo con il database delle targhe; 5. effettuare quindi interrogazioni massive al P.R.A. con costi proibitivi (milioni di euro); 6. violare con ciò il contratto con la Provincia autonoma; 7. decidere di agire per finalità proprie, divenendo titolare del trattamento, con esclusione di responsabilità per la Provincia; 8. il tutto senza alcuna ragione plausibile”;

“nell’ipotesi invece di sottrazione degli hash da parte di terzi malintenzionati, il doppio di passaggio di salting costituisce vincolo matematicamente insuperabile, dunque non c’è dubbio alcuno che il terzo sottrarrebbe dati inutilizzabili”;

“gli hash salted [...] non sono dunque riconducibili all’art. 4.1) [del Regolamento]”.

Tale linea difensiva non può essere condivisa. Affinché sia possibile rilevare il transito di un veicolo in entrata e in uscita dal territorio interessato dal progetto, è, infatti, necessario che il sistema generi medesimi identificativi (secondo valore di hash e numero progressivo ad esso associato) a partire da un medesimo numero di targa, affinché i dati relativi ai transiti di tale veicolo possano essere attribuiti a una medesima “unità di traffico”. In particolare, il primo identificativo univoco del veicolo (secondo valore di hash) è calcolato, a partire dal numero di targa di un veicolo, sulla base di funzioni di hashing (e di un insieme limitato e non variabile di salt), che sono considerate tecniche di pseudonimizzazione deboli e vulnerabili ai cc.dd. attacchi a forza bruta (cfr. il documento “Pseudonymisation techniques and best practices” pubblicato nel mese di novembre 2019 dall’Agenzia dell’Unione europea per la cibersicurezza - ENISA, spec. par. 5.1.3), mentre il secondo identificativo univoco del veicolo (numero progressivo), associato al primo identificativo univoco, è assegnato all’atto del primo transito e rimane invariabile nel corso del tempo. In tale contesto, è possibile, ad esempio, dato un determinato numero di targa, calcolare il secondo valore di hash e verificarne la presenza nel primo database (circostanza indicativa del fatto che il veicolo in questione ha effettuato almeno un transito nel territorio interessato dal progetto); in caso di presenza di tale valore di hash, è poi possibile recuperare il numero progressivo a esso associato e ricercare, nel secondo database, i dati relativi ai transiti associati a tale numero progressivo. Essendo limitato l’insieme dei numeri di targa (ad esempio, nel sistema di numerazione attualmente utilizzato in Italia, le possibili combinazioni dei numeri di targa da AA001AA a GZ999ZZ, non tutti validi o utilizzati, sono circa 75 milioni), le predette operazioni possono essere effettuate, facendo ricorso a mezzi ragionevolmente a disposizione di chiunque, oltre che su un singolo numero di targa, sul complessivo insieme dei numeri di targa. È, pertanto, tecnicamente e astrattamente possibile per il titolare o il responsabile del trattamento, nonché per eventuali soggetti terzi che per qualsiasi motivo vengano a conoscenza delle caratteristiche delle funzioni di hashing utilizzate (e dell’insieme di salt applicati) e delle informazioni sulle relazioni tra i due identificativi univoci (secondo valore di hash e numero progressivo), associare i dati relativi ai transiti ai numeri di targa dei veicoli che li hanno effettuati.

Alla luce di tutte le considerazioni che precedono, risulta accertato che la Provincia, avvalendosi di un responsabile del trattamento, abbia posto in essere un trattamento di dati personali relativi ai veicoli in transito nelle aree in cui sono stati installati i dispositivi video in questione.

D'altra parte, ancorché la Provincia abbia dichiarato in sede di memoria difensiva che "la realizzazione di informative ai sensi dell'art. 13 [del Regolamento], la qualificazione del contratto con [l'Azienda] ai sensi dell'art. 28 [del Regolamento] e le altre attività conformi al Regolamento poste in essere dalla Provincia autonoma sono riconducibili solo a un approccio prudenziale", non emerge da alcun documento in atti che l'Ente avesse posto in essere tali adempimenti soltanto in via precauzionale; può, invece, dedursi da tale circostanza come la Provincia non fosse certa delle proprie determinazioni in merito alla non riconducibilità delle informazioni raccolte alla nozione di dati personale, tanto da essersi comunque determinata ad adempiere a taluni degli obblighi previsti dal Regolamento.

3.3. La liceità del trattamento.

Il trattamento di dati personali mediante dispositivi video, da parte di soggetti pubblici, è generalmente ammesso se esso è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito lo stesso (v. art. 5, par. 1, lett. a), 6, parr. 1, lett. c) ed e), 2 e 3, del Regolamento, nonché art. 2-ter del Codice; cfr. le "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", adottate dal Comitato europeo per la protezione dei dati il 29 gennaio 2020, par. 41; v. anche le FAQ del Garante in materia di videosorveglianza, del 3 dicembre 2020, doc. web n. 9496574).

Il titolare del trattamento è tenuto, in ogni caso, a rispettare i principi in materia di protezione dei dati, fra i quali quelli di "liceità, correttezza e trasparenza" e "minimizzazione dei dati", in base ai quali i dati personali devono essere "trattati in modo lecito, corretto e trasparente nei confronti dell'interessato", nonché "adequati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. a) e c), del Regolamento).

Nel corso dell'istruttoria, la Provincia ha affermato che il trattamento di dati personali in questione si è reso necessario per poter "studiare e comprendere [i] flussi di traffico, la loro dinamica, l'orientamento, la tipologia (turistico, pendolare, di attraversamento, residenziale), la frequenza" e poi "procedere a una sostanziale rimodulazione dei flussi di traffico nella zona dolomitica" (nota del XX). Allo stato, i dispositivi video in questione non sarebbero, invece, impiegati a fini di prevenzione, indagine, accertamento e perseguimento di reati.

Il previo monitoraggio dei flussi di traffico si renderebbe necessario per poter adeguatamente motivare gli interventi della Provincia in materia, da adottarsi ai fini del conseguimento dell'obiettivo di garantire la sicurezza dei passi dolomitici, protetti dall'UNESCO, rispetto ai massivi flussi di traffico stradali che li interessano, così come stabilito con deliberazione della Giunta provinciale del 6 agosto 2019.

L'attività in questione sarebbe, altresì, necessaria ai fini dell'art. 19 del d.P.R. 22 marzo 1974, n. 381, ai sensi del quale, nell'esercizio delle funzioni ad esse spettanti in materia di paesaggio e delle altre ad esse delegate, le Province, d'intesa tra loro e previo parere del Ministero competente in materia di infrastrutture e mobilità, possono disciplinare misure per la limitazione del traffico veicolare lungo le strade che collegano i rispettivi territori.

La Provincia ha, altresì, richiamato l'art. 13 comma 7 e 227 del "Nuovo Codice della Strada" quale norma sulla base della quale può fondarsi il trattamento di dati personali in questione.

Al riguardo, deve evidenziarsi che, come affermato dalla Corte di giustizia dell'unione europea, ai

sensi dell'art. 52, par. 1, prima frase, della Carta dei diritti fondamentali dell'Unione europea ("CDFUE"), eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti da quest'ultima - che comprendono, segnatamente, il diritto al rispetto della vita privata, garantito dall'art. 7 della Carta, e il diritto alla protezione dei dati di carattere personale, sancito dall'art. 8 della Carta - devono, infatti, essere previste dalla legge, il che implica, in particolare, che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato. In particolare, "per soddisfare il requisito di proporzionalità, che trova espressione nell'articolo 5, paragrafo 1, lettera c), del regolamento [...] la normativa su cui si fonda il trattamento deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura [prevista] e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente [i] dati contro il rischio di abusi. Tale normativa dev'essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale e, in particolare, indicare in quali circostanze e a quali condizioni una misura che preveda il trattamento di tali dati possa essere adottata, garantendo così che l'ingerenza sia limitata allo stretto necessario" (sent. C-175/20, *Valsts iemumu dienests*, 24 febbraio 2022, par. 83).

A tal proposito, la Corte ha, inoltre, affermato che la normativa recante una misura che consenta un'ingerenza siffatta deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e fissino requisiti minimi, di modo che le persone i cui dati personali siano stati trattati dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati contro i rischi di abusi (v. C-175/20, cit., par. 55; v. art. 6, par. 3, del Regolamento, nonché cons. 45 dello stesso).

Inoltre, eventuali limitazioni ai diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali (e artt. 7 e 8 della CDFUE) "possono [...] essere apportate, [oltre che] a condizione che, conformemente all'articolo 52, paragrafo 1, della Carta, esse siano previste dalla legge" e "rispettino il contenuto essenziale dei diritti fondamentali nonché il principio di proporzionalità. In virtù di tale principio, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a obiettivi di interesse generale riconosciuti dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. Esse devono operare nei limiti dello stretto necessario e la normativa che comporta l'ingerenza deve prevedere norme chiare e precise che disciplinano la portata e l'applicazione della misura in questione" (C-184/20, *Vyriausioji tarnybinų etikos komisija*, 1° agosto 2022, par. 64).

Analoghi principi sono stati affermati anche dalla Corte europea dei diritti dell'uomo in relazione all'ammissibilità di limitazioni al diritto al rispetto della vita privata e familiare sancito dall'art. 8 della Convenzione europea dei diritti dell'uomo, anche nei casi in cui l'ingerenza riguardi attività o condotte che si svolgono in un luogo pubblico (cfr. "Glukhin v. Russia", "application no. 11519/20", 4 luglio 2023, parr. 64, 75 e 77; "Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland", "application no. 931/13", 27 giugno 2017, parr. 129-131; "Peck v. United Kingdom", "Application no. 44647/9", 28 gennaio 2003, punto 59; "Copland v. United Kingdom", "Application no. 62617/00", 3 aprile 2007, par. 46).

In aderenza a tale quadro giuridico e alla giurisprudenza delle due Corti, l'art. 6, parr. 2 e 3, del Regolamento precisa che la base su cui si fonda il trattamento dei dati di cui al par. 1, lettere c) ed e), deve essere stabilita dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento, che deve determinare la finalità del trattamento, nonché contenere disposizioni specifiche per adeguare l'applicazione delle norme del Regolamento, fermo restando che il diritto dell'Unione o degli Stati membri deve, in ogni caso, perseguire un obiettivo d'interesse pubblico ed essere proporzionato all'obiettivo legittimo perseguito.

In attuazione di quanto previsto dall'art. 6, parr. 2 e 3, del Regolamento, il legislatore nazionale ha precisato che la base giuridica prevista dall'art. 6, par. 3, lett. b), del Regolamento, ovvero "il diritto

dello Stato membro cui è soggetto il titolare del trattamento” e su cui “si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), [dell’art. 6 del Regolamento], è costituita “da una norma di legge o di regolamento o da atti amministrativi generali” (v. art. 2-ter, comma 1, del Codice).

Ciò premesso, con riguardo al caso di specie, si osserva che la Provincia non ha comprovato la sussistenza di un quadro giuridico qualitativamente idoneo a giustificare il trattamento dei numeri di targa dei veicoli in transito per le finalità di trattamento prospettate.

In particolare, si osserva che la Provincia ha fatto, anzitutto, riferimento agli artt. 13, comma 7 e 227 del d.lgs. 30 aprile 1992, n. 285 (Nuovo codice della strada), che non contemplano, tuttavia, la possibilità di acquisire i numeri di targa dei veicoli in transito e tracciare la frequenza del passaggio e il percorso effettuato da specifici veicoli. Né la Provincia ha fatto riferimento a specifiche “direttive impartite dal Ministero dell’ambiente e della tutela del territorio, sentito il Ministero delle infrastrutture e dei trasporti” che, ai fini di tali disposizioni, contemplerebbero i trattamenti di dati personali in questione.

La Provincia ha, altresì, fatto presente che l’iniziativa in questione è oggetto della deliberazione della Giunta provinciale n. 683 del 6 agosto 2019, con oggetto “Approvazione dello schema di convenzione tra la Provincia [...] di Trento e la Provincia [...] di Bolzano per la gestione di un sistema di monitoraggio strutturale del traffico veicolare sui passi dolomitici”, adottata ai fini dell’art. 19 del d.P.R. 22 marzo 1974, n. 381. Tale deliberazione ha ad oggetto l’“Approvazione dello schema di convenzione tra la Provincia [...] di Trento e la Provincia [...] di Bolzano per la gestione di un sistema di monitoraggio strutturale del traffico veicolare sui passi dolomitici”. Mediante tale convenzione, le due Province, al fine di “adottare misure più idonee [rispetto all’accesso programmato cadenzato], [hanno inteso avviare] un percorso di raccolta sistematica di dati per il monitoraggio del traffico attraverso quattro passi dolomitici”. Lo scopo “di tale monitoraggio è quello di poter costruire, per l’intero arco della stagione, una matrice O/D [, vale a dire origine/destinazione,] sul traffico veicolare che attualmente percorre i passi dolomitici, mediante un sistema di telecamere e la realizzazione di un software specifico, associato ad un relativo database, che rimarrà di proprietà delle due Amministrazioni, che permetterà la classificazione in almeno 4 categorie di veicoli (moto, auto, bus, altro) e in diverse classi di velocità nonché la possibilità di un’eventuale omologazione per fini sanzionatori”. Il “progetto di monitoraggio strutturale a partire dall’estate 2019, consiste nel montaggio e gestione di un sistema di 24 telecamere fisse per un periodo di 8 anni [...]”. Si legge, inoltre, che “la gestione del sistema di monitoraggio sarà in capo alla Provincia di Bolzano, mentre il flusso dati sarà accessibile da entrambe le Province. Il sistema rimarrà di proprietà delle due amministrazioni”.

La norma di legge cui fa riferimento detta deliberazione, vale a dire l’art. 19 del d.P.R. 22 marzo 1974, n. 381, si limita, tuttavia, a contemplare la possibilità di “disciplinare misure per la limitazione del traffico veicolare lungo le strade che collegano i rispettivi territori”, prevedendo un generico obbligo di motivazione dei provvedimenti in tal senso assunti, ma senza alcuno specifico riferimento alla necessità di tracciare i tragitti effettuato da specifici veicoli, mediante tecnologie di rilevamento del numero di targa.

In tale quadro, né la Deliberazione della Giunta della Provincia di Bolzano n. 683 del 6 agosto 2019 né la correlata Deliberazione della Giunta della Provincia di Trento n. 1192 del 12 agosto 2019 possono ritenersi adeguate in termini di qualità della base giuridica (v. art. 6, par. 3, del Regolamento), atteso che esse non disciplinano in maniera puntuale le tipologie di dati oggetto del trattamento, i periodi di conservazione dei dati e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto. In particolare, le deliberazioni non fanno alcun esplicito riferimento alla raccolta e al trattamento dei dati relativi al numero di targa e alla loro conservazione per un arco temporale di due anni al fine di poter ricostruire i percorsi effettuati dai veicoli, rinvenendosi unicamente un generico riferimento alla creazione di una “una matrice O/D [origine/destinazione] sul traffico veicolare che attualmente percorre i passi dolomitici”. Tali aspetti sono stati, infatti, definiti dalla Provincia unicamente con atti organizzativi

interni e nell'ambito dei rapporti contrattuali con il responsabile del trattamento. Né può accogliersi l'argomento, prospettato dalla Provincia in sede di memoria difensiva, in base al quale la "[...] delibera di Giunta della [...] Provincia [...] prescrive sia la necessità di costruzione della matrice O/D (che postula il riconoscimento di uno stesso veicolo nel passaggio in almeno due postazioni diverse, dunque utilizzo di videocamere) sia la necessità di classificazione dei veicoli (che, associata alla matrice O/D, postula l'utilizzo di videocamere), sia la diversa classe di velocità (che ugualmente richiede videocamere)", atteso che, come sopra evidenziato, la normativa che comporta un'ingerenza sul diritto alla protezione dei dati deve contenere previsioni chiare e precise che disciplinino la portata e l'applicazione della stessa, soddisfacendo i requisiti di qualità previsti dal Regolamento, così risultando il trattamento prevedibile per gli interessati. Tali requisiti non possono considerarsi soddisfatti ove, come sostenuto dalla Provincia, il trattamento sia soltanto deducibile dalla complessiva formulazione della disposizione su cui lo stesso si fonda.

La Provincia, nell'ambito delle proprie memorie difensive, ha, altresì, affermato che, nella denegata ipotesi in cui si dovesse ritenere sussistente un trattamento di dati personali, occorre considerare che "la base [giuridica del trattamento] è quella dell'art. 6.1.e) [del Regolamento], per cui, a mente dell'art. 6.3, non occorre né che la disposizione di riferimento indichi la finalità, essendo sufficiente che essa sia "necessaria" al compito di pubblico interesse, né soprattutto che indichi le categorie di dati personali e gli altri elementi del trattamento, come chiaramente si deduce dall'utilizzo, all'art. 6.3 del verbo "potere", peraltro al condizionale "potrebbe contenere ecc.". Allo stesso modo, il comma 1-bis dell'art. 2-ter [del Codice] conferma la liceità del trattamento".

A tal proposito, occorre evidenziare che, come affermato dalla Corte di giustizia dell'Unione europea, "il trattamento lecito di dati personali [...] sulla base dell'articolo 6, paragrafo 1, lettera e), del RGPD presuppone non solo che si possa ritenere che [i titolari del trattamento] svolgano un compito di interesse pubblico, ma anche che i trattamenti di dati personali per l'esecuzione di un siffatto compito si fondino su una base giuridica prevista all'articolo 6, paragrafo 3, di tale regolamento" (sentenza del 20 ottobre 2022, Koalitsia «Demokraticzna Bulgaria – Obedinenie» - C306/21, par. 48-52). In particolare, la base giuridica del trattamento di cui all'art. 6, par. 1, lett. e), del Regolamento, "conformemente all'articolo 6, paragrafo 3, del RGPD, in combinato disposto con il considerando 45 di quest'ultimo [...] deve essere stabilita dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento. Inoltre, il diritto dell'Unione o il diritto degli Stati membri deve perseguire un obiettivo di interesse pubblico ed essere proporzionato all'obiettivo legittimo perseguito. Il combinato disposto dell'articolo 6, paragrafo 1, lettera e), del RGPD e dell'articolo 6, paragrafo 3, di tale regolamento richiede quindi una base giuridica, segnatamente nazionale, per il trattamento dei dati personali da parte dei titolari del trattamento che agiscono nell'esecuzione di un compito di interesse pubblico o di un compito connesso all'esercizio di pubblici poteri" (sentenza del 2 marzo 2023, C-268/21 - Norra Stockholm Bygg, par. 30-32; v. anche sentenza del 30 marzo 2023, C-34/21 - Hauptpersonalrat der Lehrerinnen und Lehrer, par. 87). Pertanto, in assenza di specifiche disposizioni dell'ordinamento (cfr. art. 2-ter, comma 1, del Codice) che contemplino e disciplinino con i necessari requisiti di qualità i trattamenti che si rendono necessari per l'esecuzione di un compito d'interesse pubblico o l'esercizio di pubblici poteri, il titolare del trattamento non può genericamente invocare la base giuridica di cui all'art. 6, par. 1, lett. e), del Regolamento (cfr. l'art. 2-ter, 1-bis, del Codice, che, nel consentire il trattamento "necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti", prescrive comunque "il rispetto dell'articolo 6 del Regolamento").

Ciò chiarito in merito ai requisiti di qualità della base giuridica, occorre evidenziare che un trattamento di dati personali può rinvenire la propria base giuridica nell'art. 6, par. 1, lett. e), del Regolamento se e nella misura in cui esso sia "necessario" per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del

trattamento, condizione che deve essere esaminata unitamente al principio di minimizzazione dei dati sancito all'art. 6, par. 1, lett. c), del Regolamento, in base al quale i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Ciò in quanto, come sopra evidenziato, conformemente ai già richiamati art. 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, di cui agli artt. 7 e 8 della Carta, possono essere soggetti a limitazioni solo a condizione che le stesse siano previste dalla legge e che rispettino il contenuto essenziale dei diritti fondamentali nonché il principio di proporzionalità, espressamente richiamato dall'art. 6, par. 3, del Regolamento. In virtù di tale principio, dette limitazione devono essere necessarie e rispondere effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui, operando nei limiti dello stretto necessario.

Pertanto, al fine di determinare se un trattamento sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, occorre verificare in particolare se, alla luce della gravità dell'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, causata dal trattamento, quest'ultima risulti giustificata e, in particolare, proporzionata, ai fini della realizzazione degli obiettivi perseguiti. Come evidenziato dal cons. 39 del Regolamento, tale requisito di necessità non è soddisfatto quando l'obiettivo di interesse generale considerato può ragionevolmente essere raggiunto in modo altrettanto efficace mediante altri mezzi meno pregiudizievoli per i diritti fondamentali degli interessati, in particolare per i diritti al rispetto della vita privata e alla protezione dei diritti personali garantiti agli articolo 7 e 8 della Carta, atteso che le deroghe e le restrizioni al principio della protezione di simili dati devono avere luogo nei limiti dello stretto necessario (v. Corte di giustizia dell'Unione europea, sentenze C-184/20, Vyriausioji tarnybinų etikos komisija, del 1° agosto 2022, par. 73, 82, 85, 93, 94, 98, 99; C-439/19, Latvijas Republikas Saeima, del 22 giugno 2021, par. 99, 105, 106 e 113).

Nel caso di specie, non emerge dalla documentazione in atti che la Provincia abbia effettuato specifiche e preliminari valutazioni in merito all'effettiva necessità del trattamento di dati personali in questione e alla proporzionalità dello stesso all'obiettivo perseguito (v. art. 6, par. 3, del Regolamento), non essendo astrattamente possibile escludere che vi fossero strumenti e soluzioni sufficientemente efficaci, ma meno impattanti per i diritti e le libertà degli interessati, per poter motivare gli eventuali provvedimenti di limitazione del traffico eventualmente assunti ai sensi del citato art. 19 del d.P.R. 22 marzo 1974, n. 381. D'altra parte, come messo in evidenza dal Comitato europeo per la protezione dei dati, ancorché in un diverso contesto, "i dati relativi all'ubicazione sono particolarmente atti a fornire indicazioni sulle abitudini di vita degli interessati. I viaggi effettuati hanno la particolare caratteristica di permettere di risalire al luogo di lavoro e di residenza, nonché ai centri di interesse (svago) del conducente" ("Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità", 9 marzo 2021, pag. 17). Soltanto in sede di memoria difensiva la Provincia ha, infatti, sostenuto che "la realtà è che non esiste soluzione tecnica alternativa affidabile, quella applicata rispondendo allo stato dell'arte [...] Ogni altra soluzione alternativa (es. interviste agli autisti; indagini a domicilio; interviste telefoniche; questionari postali; collaborazione con gestori telefonici) è certamente peggiore, poiché non solo postulerebbe una straordinaria ricerca di dati personali, successivi trattamenti massivi, talvolta neppure possibili o neppure pertinenti, e comunque ingerenze ingiustificate nella sfera personale, ma avrebbe anche costi proibitivi", affermando, altresì, che sarebbe "onere di codesto Ufficio [del Garante] provare diversamente". Deve, invece, rammentarsi che, in ossequio al principio di responsabilizzazione (cfr. artt. 5, par. 2, e 24 del Regolamento), che informa l'intera disciplina europea in materia di protezione dei dati, è il titolare del trattamento che deve assicurare, prima di dare avvio al trattamento, il rispetto dei principi in materia di protezione dei dati, tra cui quelli di "minimizzazione dei dati" (art. 5, comma 1, lett. c), del Regolamento, che, come detto, si riflette nel requisito della "necessità" del trattamento nelle basi giuridiche di cui all'art. 6, par. 1, lett. da b) a e), del medesimo Regolamento) ed "essere in

grado di provarlo”.

Da ultimo, quanto alla circostanza che, come dichiarato, i dati relativi ai veicoli in transito possano essere trattati latu sensu per “analisi statistiche”, occorre rilevare che, ancorché tale finalità di trattamento non sia stata specificamente invocata dalla Provincia, non risulta in ogni caso comprovata la sussistenza di un’idonea base giuridica che potesse giustificare un trattamento di tali per finalità statistiche, non avendo la Provincia indicato alcuna norma di legge, o, nei casi previsti dalla legge, di regolamento, idonea per rango e qualità, che espressamente prevedesse tale trattamento, disciplinandone le caratteristiche essenziali, né l’applicabilità delle regole deontologiche di settore (cfr. artt. 6, par. 1, lett. a), e parr. 2 e 3, e 89 del Regolamento, nonché 2-ter, 2-quater, comma 4, e Capo III del Codice).

Alla luce di tutte le considerazioni che precedono, risulta accertato che la Provincia ha posto in essere il trattamento dei dati personali in questione, relativi ai veicoli in transito, mediante l’impiego di dispositivi video installati sulla pubblica via, in maniera non conforme al principio di liceità, correttezza e trasparenza, e in assenza di un’idonea base giuridica, in violazione degli artt. 6, par. 1, lett. c) ed e), e parr. 2 e 3, del Regolamento, nonché 2-ter del Codice.

3.4. Il principio di limitazione della conservazione

In base al principio di “limitazione della conservazione”, i dati personali devono essere conservati in una forma che consenta l’identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (art. 5, par. 1, lett. e), del Regolamento).

La Provincia ha dichiarato di conservare i dati personali pseudonimizzati per un periodo di due anni dalla data della raccolta, essendo “possibile interrogare il software per creare report sulla base di dati storici fino a 2 anni”.

Tale periodo di conservazione estremamente esteso non può considerarsi proporzionato rispetto alle finalità del trattamento perseguite, atteso che, una volta rilevate le caratteristiche d’interesse di ciascun veicolo transitato (classe; classe di velocità; origine e destinazione) e acquisite le pertinenti informazioni ai fini dell’elaborazione dei dati aggregati, non vi è alcuna ragione per conservare il dato relativo alla targa, ancorché pseudonimizzato, per un arco temporale così lungo, esponendo gli interessati a un significativo rischio per i propri diritti e le proprie libertà fondamentali, derivante dal fatto che i propri spostamenti sul territorio possono essere sistematicamente tracciati e ricostruiti.

Pertanto, non vi è evidenza in atti che oggetto di cancellazione al decorso di tale arco temporale siano anche i dati relativi agli identificativi univoci (secondo valore di hash e numero progressivo) dei veicoli transitati nel territorio di riferimento, la cui conservazione, anche a fronte della cancellazione delle informazioni relative ai singoli transiti effettuati, è idonea a rendere nota la circostanza che quantomeno un transito sia stato effettuato.

Per tali ragioni, la Provincia ha agito in maniera non conforme al principio di “limitazione della conservazione”, in violazione dell’art. 5, par. 1, lett. e), del Regolamento.

3.5. La trasparenza nei confronti degli interessati.

Nel rispetto del principio di “liceità, correttezza e trasparenza”, il titolare del trattamento deve adottare misure appropriate per fornire all’interessato, prima di iniziare il trattamento, tutte le informazioni richieste dal Regolamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (artt. 5, par. 1, lett. a), 12 e 13 del Regolamento).

Allorquando siano impiegati dispositivi video, il titolare del trattamento, oltre a rendere l’informativa di primo livello mediante apposizione di segnaletica di avvertimento in prossimità della zona sottoposta a videosorveglianza, deve fornire agli interessati anche delle “informazioni di secondo

livello”, che devono “contenere tutti gli elementi obbligatori a norma dell’articolo 13 del [Regolamento]” ed “essere facilmente accessibili per l’interessato, ad esempio attraverso un pagina informativa completa messa a disposizione in uno snodo centrale [...] o affissa in un luogo di facile accesso” (“Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video” del Comitato europeo per la protezione dei dati, adottate il 29 gennaio 2020, in particolare par. 7; ma si veda già il “Provvedimento in materia di videosorveglianza” del Garante dell’8 aprile 2010, doc. web n. 1712680, in particolare par. 3.1; da ultimo, v. le FAQ del Garante in materia di videosorveglianza, doc. web n. 9496574, n 4; cfr., altresì, provv.ti 29 aprile 2025, n. 244, doc. web n. 10144974; 10 aprile 2025, n. 201, doc. web n. 10139433; 27 marzo 2025, n. 168, doc. web n. 10138999; 19 dicembre 2024, n. 805, doc. web n. 10107263; 22 febbraio 2024, n. 100, doc. web n. 9990659; 11 gennaio 2024, n. 5, doc. web n. 9977020 e il relativo comunicato stampa del 25 gennaio 2024, doc. web n. 9977299; 20 ottobre 2022, n. 341, doc. web n. 9831369; 28 aprile 2022, n. 162, doc. web n. 9777974; 7 aprile 2022, n. 119, doc. web n. 9773950; 16 settembre 2021, n. 327, doc. web n. 9705650 e 11 marzo 2021, n. 90, doc. web n. 9582791).

Le informazioni di primo livello (cartello di avvertimento) “dovrebbero comunicare i dati più importanti, ad esempio le finalità del trattamento, l’identità del titolare del trattamento e l’esistenza dei diritti dell’interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento” (Linee guida del Comitato, cit., par. 114). Inoltre, la segnaletica deve contenere anche quelle informazioni che potrebbero risultare inaspettate per l’interessato. Potrebbe trattarsi, ad esempio, della trasmissione di dati a terzi, in particolare se ubicati al di fuori dell’UE, e del periodo di conservazione. Se tali informazioni non sono indicate, l’interessato dovrebbe poter confidare nel fatto che vi sia solo una sorveglianza in tempo reale (senza alcuna registrazione di dati o trasmissione a soggetti terzi) (Linee guida del Comitato, cit., par. 115). La segnaletica di avvertimento di primo livello deve contenere un chiaro riferimento al secondo livello di informazioni, ad esempio indicando un sito web sul quale è possibile consultare il testo dell’informativa estesa.

Per quanto concerne la trasparenza del trattamento, deve preliminarmente osservarsi che gli interessati dai trattamenti in questione sono non solo i proprietari dei veicoli rilevati ma anche gli eventuali diversi conducenti degli stessi, in caso di veicoli noleggiati o comunque concessi in uso ad altro titolo a terzi, anche in ambito familiare. Inoltre, interessati dai trattamenti sono anche tutte le altre persone che, indipendentemente dall’acquisizione del numero di targa, compaiono nei filmati, che, ancorché per una ridotta frazione temporale, vengono acquisiti con i dispositivi video collocati nella pubblica via ai fini della lettura del numero di targa.

La Provincia ha depositato in atti copia dell’informativa di primo livello (cartello di avvertimento) che sarebbe stata fornita agli interessati (v. all. XX alla nota del XX, cit.). Tale informativa non risulta, tuttavia, conforme ai requisiti previsti dagli artt. 5, par. 1, lett. a), e 13 del Regolamento, in quanto:

non menziona la Provincia di Trento quale contitolare del trattamento (cfr. art. 13, par. 1, lett. a), del Regolamento; v. anche par. 3.6 del presente provvedimento);

indica una finalità del trattamento (“sicurezza stradale”) del tutto inconferente rispetto a quella asseritamente perseguita (cfr. art. 13, par. 1, lett. c), del Regolamento);

non menziona i diritti degli interessati di cui agli artt. 15-22 del Regolamento (cfr. art. 13, par. 2, lett. b), del Regolamento);

non fornisce informazioni sugli impatti più consistenti del trattamento, con particolare riguardo alla lettura automatizzata delle targhe dei veicoli in transito (cfr. art. 5, par. 1, lett. a), del Regolamento);

non fa riferimento al periodo di conservazione dei dati pari a due anni dalla raccolta, in quanto informazione che potrebbe risultare inaspettata per gli interessati (cfr. art. 5, par. 1, lett. a), del Regolamento);

non contiene un chiaro riferimento al secondo livello di informazioni, ad esempio indicando un sito web sul quale è possibile consultare il testo dell'informativa estesa (cfr. art. 5, par. 1, lett. a), del Regolamento). Non rileva, a tal riguardo, quando sostenuto dalla Provincia con la propria memoria difensiva in merito alla circostanza che "il cartello informativo inizialmente utilizzato [...] era quello pro tempore suggerito [dal] Garante [, ovvero quello di cui al provvedimento generale in materia di videosorveglianza dell'8 aprile 2010,], che non recava link [all'informativa di secondo livello]"; ciò in quanto le indicazioni in merito agli elementi che devono comporre l'informativa di primo livello sono state fornite dal Comitato europeo per la protezione dei dati fin dal XX con le richiamate Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, antecedentemente al periodo in cui la Provincia ha installato i dispositivi video per l'esecuzione del progetto (XX); quanto alla circostanza che, come affermato sempre in sede di memoria difensiva, "e che "l'art. 13 [del Regolamento] non contempla l'inserimento del suddetto link tra i requisiti essenziali dell'informativa, dunque esso può ragionevolmente essere considerato elemento opportuno, ma non necessario", deve osservarsi che, di regola, il titolare del trattamento deve fornire agli interessati tutte le informazioni di cui all'art. 13 del Regolamento e che lo stesso può beneficiare della possibilità di rendere agli stessi un'informativa stratificata, composta da un'informativa semplificata di primo livello e una estesa di secondo livello, solo a condizione che l'informativa di primo livello contenga un rinvio a quella di secondo livello, consentendo così agli interessati, ove lo desiderino, di poter acquisire tutte le informazioni relative al trattamento (v. le richiamate Linee guida 3/2019, parr. 111 e 117, ove si evidenzia che "i titolari del trattamento possono seguire un approccio scalare, optando per una combinazione di metodi al fine di assicurare la trasparenza [...]. Per quanto riguarda la videosorveglianza, le informazioni più importanti devono essere indicate sul segnale di avvertimento stesso (primo livello), mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello)", fermo restando che "la segnaletica di avvertimento di primo livello deve contenere un chiaro riferimento a tale secondo livello di informazioni").

La Provincia ha, altresì, dichiarato di aver sostituito gli iniziali cartelli di avvertimento con "gli attuali cartelli contenenti l'informativa di primo livello [, che] sono stati installati tra il XX ed il XX, in sostituzione dei precedenti cartelli", ovvero successivamente all'avvio dell'istruttoria da parte dell'Autorità (v. all. XX alla nota del XX).

Anche tale nuova versione dell'informativa di primo livello sul trattamento dei dati non risulta pienamente conforme ai requisiti previsti dall'art. 5, par. 1, lett. a), e 13 del Regolamento, in quanto:

non menziona la Provincia di Trento quale contitolare del trattamento (cfr. art. 13, par. 1, lett. a), del Regolamento; v. anche par. 3.6 del presente provvedimento);

menziona erroneamente il Servizio Strade della Provincia quale titolare del trattamento e la stessa Provincia quale Responsabile della protezione dei dati (cfr. art. 13, par. 1, lett. a) e b), del Regolamento

non menziona i diritti degli interessati di cui agli artt. 15-22 del Regolamento (cfr. art. 13, par. 2, lett. b), del Regolamento);

non fa riferimento al periodo di conservazione dei dati pari a due anni dalla raccolta, in quanto informazione che potrebbe risultare inaspettata per gli interessati (cfr. art. 5, par. 1, lett. a), del Regolamento);

Quanto all'informativa di secondo livello sul trattamento dei dati personali, la Provincia ha dichiarato che "l'informativa di secondo livello è stata resa disponibile agli interessati presso gli Uffici tecnici della Ripartizione Servizio strade della Provincia Autonoma di Bolzano a far tempo dal 25 ottobre 2019 [...]" e che "nell'ambito dell'attività di accountability è stata quindi effettuata una revisione del testo, che ha dato luogo a una seconda versione aggiornata, in data XX, messa a disposizione presso gli stessi Uffici [...]". Tale versione "è stata altresì messa a disposizione in data XX sia presso gli uffici, sia online al link <https://www.provincia.bz.it/turismo-mobilita/strade/manutenzione/monitoraggio-del-traffico.asp>, sul sito web istituzionale del Servizio strade della Provincia Autonoma di Bolzano".

Con riguardo alla prima versione dell'informativa estesa, fornita a partire dal 25 ottobre 2019, si osserva che gli interessati vengono informati della circostanza che "non vi inoltre la possibilità di risalire al dato personale successivamente alla sua conversione", affermazione che non riflette le effettive caratteristiche del trattamento, atteso che, come sopra illustrato, il responsabile del trattamento, che agisce per conto della Provincia, è in possesso delle informazioni necessarie per associare gli stessi ai numeri di targa, trattandosi di meri dati pseudonimizzati. Ugualmente, per le medesime ragioni, non risulta corretto che "il trattamento di dati personali è dunque di minima durata", in quanto "il codice alfanumerico targa viene immediatamente anonimizzato", con "impossibilità di risalire alla targa originaria", e che "il periodo di conservazione del dato personale è minim[o]", anche tenuto conto che, come sopra evidenziato, i dati pseudonimizzati vengono conservati per un periodo di due anni. Tali affermazioni concretizzano una violazione degli artt. 5, par. 1, lett. a), e 13, par. 2, lett. a), del Regolamento.

Inoltre, al par. 6 dell'informativa si afferma che "il particolare funzionamento del sistema di crittografia, che trasforma il dato personale immediatamente in dato anonimo mediante sistema di criptazione, non vi è trattamento se non a livello meramente teorico su base software" e che, pertanto, "non risulta quindi un trattamento tale da consentire l'esercizio dei diritti dell'interessato". Alla luce delle precedenti considerazioni in merito alla piena sussistenza di un trattamento di dati personali per un esteso arco temporale di due anni, tale scorretta affermazione configura una violazione degli artt. 5, par. 1, lett. a) e 13, par. 2, lett. b), del Regolamento.

Si rileva, altresì, che il diritto di opposizione di cui all'art. 21 del Regolamento non è stato portato esplicitamente portato all'attenzione degli interessati e non è stato presentato chiaramente e separatamente da qualsiasi altra informazione, risultando violato anche l'art. 21, par. 4, del Regolamento.

L'informativa in questione non indica, inoltre, chiaramente gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali, non essendovi alcun riferimento al fornitore che, in qualità di responsabile del trattamento, tratta i dati personali per conto della Provincia, risultando, pertanto, violato l'art. 13, par. 1, lett. e), del Regolamento.

Su un piano più generale, deve poi osservarsi che non può considerarsi conforme agli artt. 12, par. 1, e 13 del Regolamento, la circostanza che tale versione dell'informativa completa di secondo livello sia stata messa a disposizione degli interessati soltanto in versione cartacea presso "gli Uffici tecnici della Ripartizione Servizio strade della Provincia Autonoma di Bolzano", senza pubblicare il testo della stessa anche sul sito web istituzionale della Provincia. L'art. 12, par. 1, del Regolamento prevede, infatti, che l'informativa di cui all'art. 13 del Regolamento debba essere "facilmente accessibile" agli interessati. A tal riguardo, il Comitato europeo per la protezione dei dati ha affermato che "le informazioni di secondo livello devono essere facilmente accessibili per l'interessato, ad esempio attraverso un pagina informativa completa messa a disposizione in uno snodo centrale (sportello informazioni, reception, cassa, ecc.) o affissa in un luogo di facile accesso" ("Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", adottate il XX, par. XX), ma sul presupposto che tale snodo centrale si trovi in prossimità della zona soggetta a videosorveglianza. Diversamente, allorquando, come nel caso di

specie, i dispositivi di videosorveglianza siano distribuiti su aree di vaste dimensioni e distanti dalla sede del titolare del trattamento, l'informativa di primo livello deve rimandare necessariamente a un'informativa di secondo livello reperibile online, in maniera tale che gli interessati possano facilmente accedere alla stessa, senza doversi fisicamente recare presso la sede del titolare del trattamento. Risultano, pertanto, complessivamente violati, nel periodo intercorrente tra la data di inizio del trattamento e il XX, data in cui l'informativa è stata pubblicata online, gli artt. 12, par. 1, e 13 del Regolamento.

Quanto all'informativa sul trattamento dei dati, messa a disposizione degli interessati a partire dal XX e pubblicata sul sito web istituzionale della Provincia a partire dal XX, successivamente all'avvio dell'istruttoria da parte dell'Autorità, si rileva che anche tale versione del documento riporta scorrettamente che "non vi è inoltre possibilità di risalire al dato personale", che "il trattamento di dati personali è dunque di minima durata: mediante una apposita funzione crittografica, il codice alfanumerico della targa viene immediatamente anonimizzato e utilizzato a fini statistici", che "la funzione crittografica [...] assicura l'impossibilità di risalire alla targa originaria successivamente alla sua conversione" e che "il periodo di conservazione del dato personale è minimo, secondo il tempo tecnicamente necessario alla trasformazione della targa del veicolo in transito in un codice crittografato (60 secondi)". Tali affermazioni concretizzano una violazione degli artt. 5, par. 1, lett. a), e 13, par. 2, lett. a), del Regolamento.

Inoltre, al par. 6 dell'informativa si afferma che "il dato personale raccolto viene immediatamente trasformato in dato anonimo a fini statistici, il che potrebbe comportare deroghe all'esercizio dei diritti a Lei spettante in qualità di interessato/a.". Alla luce delle precedenti considerazioni in merito alla piena sussistenza di un trattamento di dati personali per un esteso arco temporale di due anni, tale scorretta affermazione configura una violazione degli artt. 5, par. 1, lett. a) e 13, par. 2, lett. b), del Regolamento.

Si rileva, altresì, che il diritto di opposizione di cui all'art. 21 del Regolamento non è stato portato esplicitamente portato all'attenzione degli interessati e non è stato presentato chiaramente e separatamente da qualsiasi altra informazione, risultando violato anche l'art. 21, par. 4, del Regolamento.

L'informativa in questione non indica, inoltre, chiaramente gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali, non essendovi alcun riferimento al fornitore che, in qualità di responsabile del trattamento, tratta i dati personali per conto della Provincia, risultando, pertanto, violato l'art. 13, par. 1, lett. e), del Regolamento.

L'insufficiente trasparenza nei confronti degli interessati risulta poi complessivamente aggravata dalla circostanza che, come evidenziato nel precedente par. 3.2, la base giuridica sulla quale è stato fondato il trattamento non può considerarsi qualitativamente idonea a soddisfare i requisiti previsti dal quadro giuridico europeo e nazionale in materia di protezione dei dati, non contenendo la stessa una puntuale disciplina e descrizione dei dati oggetto di trattamento, dei soggetti interessati e delle operazioni di trattamento consentite.

Alla luce di tutte le considerazioni che precedono, deve concludersi che:

- dalla data di attivazione dei dispositivi video fino ad XX, periodo in cui sono stati installati i nuovi cartelli contenenti l'informativa di primo livello, contenenti indicazioni sulle modalità con cui poter consultare l'informativa di secondo livello, la Provincia non ha adempiuto agli obblighi informativi nei confronti degli interessati (proprietari/conducenti dei veicoli/altri soggetti ripresi), avendo, pertanto agito in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento;
- a partire dal XX, data i cui sono stati installati i nuovi cartelli contenenti l'informativa di

primo livello, la Provincia ha fornito agli interessati (proprietari/conducenti dei veicoli/altri soggetti ripresi) un'informativa di primo livello non del tutto idonea, in violazione degli artt. 5, par. 1, lett. a), 13, par. 1, lett. a) e b), e par. 2, lett. b), del Regolamento, nonché un'inidonea informativa di secondo livello non del tutto idonea, in violazione degli artt. 5, par. 1, lett. a), e 13, parr. 1, lett. e) e 2, lett. a) e b), e 21, par. 4, del Regolamento.

3.6. Il rapporto di contitolarità di trattamento con la Provincia Autonoma di Trento.

Ai sensi dell'art. 4, par. 1, n. 7), del Regolamento, il titolare 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 di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, "essi sono contitolari del trattamento" e devono "determina[re] in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati" (art. 26, par. 1, del Regolamento). L'accordo tra i contitolari "riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati" e il "contenuto essenziale dell'accordo [deve essere] messo a disposizione dell'interessato" (art. 26, par. 2, del Regolamento).

Come, infatti, chiarito dalla Corte di giustizia dell'Unione europea, "una persona fisica o giuridica che influisca, per scopi che le sono propri, sul trattamento di dati personali e partecipi pertanto alla determinazione delle finalità e dei mezzi di tale trattamento può essere considerata titolare del trattamento, ai sensi dell'articolo 4, punto 7, del RGPD" (sentenze C-604/22, IAB Europe, del 7 marzo 2024, par. 57, e C 25/17, Jehovan todistajat, 10 luglio 2018, par. 68). Quindi, "conformemente all'articolo 26, paragrafo 1, del RGPD, si è in presenza di «contitolari del trattamento» allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento" (sentenze C-604/22, cit., par. 57, e C 683/21, Nacionalinis visuomens sveikatos centras, del 5 dicembre 2023, par. 40).

Dall'istruttoria è emerso che i dispositivi video in questione sono stati collocati anche nel territorio della Provincia Autonoma di Trento, in virtù di una convenzione stipulata tra le due Province.

Nella convenzione si legge che il database creato nell'ambito del progetto "rimarrà di proprietà delle due Amministrazioni", che "la gestione del sistema di monitoraggio sarà in capo alla Provincia di Bolzano", che "il flusso dati sarà accessibile da entrambe le Province" e che "il sistema rimarrà di proprietà delle due amministrazioni" (v. Deliberazione della Giunta della Provincia di Bolzano n. 683 del 6 agosto 2019 e Deliberazione della Giunta della Provincia di Trento n. 1192 del 12 agosto 2019). La Provincia di Trento, che ha cofinanziato il progetto, ha, pertanto, il diritto di chiedere alla Provincia di ricevere i dati di output aggregati.

Sulla base di tali elementi, deve ritenersi che, stipulando la predetta convenzione, co-finanziando il progetto (nella misura del 50%) e attuando lo stesso nei rispettivi territori, al fine di ottenere informazioni aggregate sui flussi veicolari effettuati negli stessi, le due Province abbiano agito in qualità di contitolari del trattamento.

Come, infatti, chiarito dal Comitato europeo per la protezione dei dati, "il criterio generale per la

sussistenza della contitolarità di trattamento è la partecipazione congiunta di due o più soggetti nella definizione delle finalità e dei mezzi di un'operazione di trattamento. La partecipazione congiunta può assumere la forma di una decisione comune, presa da due o più soggetti [...]" ("Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", adottate il 7 luglio 2021, par. 53). A tal fine, "un criterio importante è che il trattamento non sarebbe possibile senza la partecipazione di entrambi i soggetti, nel senso che i trattamenti svolti da ciascun soggetto sono tra loro indissociabili, ovverosia indissolubilmente legati". Nel caso di specie, cofinanziando il progetto, autorizzando la Provincia di Bolzano ad affidare i lavori anche per proprio conto e a installare i dispositivi video nel proprio territorio, la Provincia di Trento ha reso possibile il complessivo trattamento di dati personali nell'ambito del progetto, che, in assenza di una sua collaborazione con la Provincia di Bolzano, non avrebbe potuto aver luogo.

Ancorché nel corso dell'istruttoria entrambe le Province abbiano sostenuto che tutte le decisioni relative alla finalità e ai mezzi del trattamento siano state assunte unicamente dalla Provincia di Bolzano e che la circostanza che la Provincia Autonoma di Trento abbia finanziato il progetto non sia determinate ai fini della sussistenza di una situazione di contitolarità, occorre rilevare che la convenzione è stata stipulata "per la gestione del programma di monitoraggio, per l'anno 2019 e seguenti, del traffico veicolare sui Passi dolomitici" e che la Provincia di Bolzano ha proceduto all'affidamento della fornitura, montaggio e gestione del sistema di monitoraggio, essendo "autorizzata alla firma del contratto anche per conto della Provincia di Trento", tanto che la Provincia di Bolzano "attraverso l'impresa aggiudicataria è [stata] autorizzata ad eseguire lavori di installazione del sistema di monitoraggio anche sulla rete stradale in gestione alla Provincia di Trento".

Inoltre, i risultati del progetto, in termini di dati aggregati sui flussi veicolari, arrecano benefici ad entrambe le Province, potendo le stesse accedere a tali dati e utilizzare gli stessi ai fini delle proprie politiche in materia di mobilità (cfr. le "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", cit., par. 60, ove si afferma che "[...] la contitolarità del trattamento può configurarsi anche qualora i soggetti perseguano finalità strettamente collegate o complementari. Ciò può verificarsi, ad esempio, quando esiste un vantaggio reciproco derivante dalla medesima operazione di trattamento [...]").

Giova a tal riguardo evidenziare che, come affermato dalla Corte di giustizia dell'Unione europea, l'esistenza di una responsabilità congiunta non implica necessariamente una responsabilità equivalente, per un medesimo trattamento di dati personali, dei diversi soggetti che vi partecipano. Al contrario, tali soggetti possono essere coinvolti in fasi diverse di tale trattamento e a diversi livelli, di modo che il grado di responsabilità di ciascuno di essi deve essere valutato tenendo conto di tutte le circostanze rilevanti nello specifico contesto (sentenze C-604/22, cit., par. 58, e C-25/17, cit., parr. 66 e 69; cfr. le "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", cit., par. 58). Non è, inoltre, necessario che la determinazione delle finalità e dei mezzi del trattamento debba essere effettuata mediante istruzioni scritte o incarichi da parte del titolare del trattamento. Può, quindi, essere considerata titolare del trattamento una persona fisica o giuridica che, per scopi che le sono propri, influisca sul trattamento di dati personali e partecipi, pertanto, alla determinazione delle finalità e dei mezzi di tale trattamento (v. sentenze C-604/22, cit., par. 61 e C-25/17, cit., par. 68; cfr. le "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", cit., parr. 57 e 58).

La circostanza che la Provincia di Trento non abbia accesso ai dati personali oggetto di trattamento e non conservi gli stessi in proprie banche dati è, a tal riguardo, influente. Ciò in quanto, sempre richiamando la giurisprudenza della Corte di giustizia dell'Unione europea, "la responsabilità congiunta di vari soggetti per un medesimo trattamento, ai sensi di tale disposizione, non presuppone che ciascuno di essi abbia accesso ai dati personali di cui trattasi"

(sentenza C-40/17, Fashion ID, del 29 luglio 2019, par. 69; v. anche sentenza C 25/17, cit., par. 69, e C 210/16, Wirtschaftsakademie Schleswig-Holstein, del 5 giugno 2018, par. 38; v. anche le “Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR”, cit., par. 56).

Alla luce delle considerazioni che precedono e in linea con precedenti provvedimenti dell’Autorità in ambito pubblico (v. provv.ti 24 gennaio 2024, nn. 31 e 32, doc. web n. doc. web n. 9992914 e 9992986; 13 aprile 2023, n. 122, doc. web n. 9896412), deve ritenersi che, nell’ambito del progetto in questione, le due Province abbiano trattato i dati personali in qualità di contitolari del trattamento, non avendo, tuttavia, gli stessi previamente stipulato un accordo di contitolarità del trattamento, in violazione dell’art. 26 del Regolamento.

3.7. La valutazione d’impatto sulla protezione dei dati.

In caso di rischi elevati per gli interessati - derivanti, ad esempio, dall’utilizzo di nuove tecnologie - il titolare del trattamento deve effettuare una valutazione d’impatto sulla protezione dei dati, al fine di adottare, in particolare, le misure adeguate ad affrontare tali rischi, consultando preventivamente il Garante, ove ne ricorrano i presupposti (v. artt. 35 e 36, par. 1, del Regolamento).

Nel caso di specie, la Provincia non ha comprovato di aver redatto una valutazione d’impatto sulla protezione dei dati prima di iniziare il trattamento in questione.

Tale valutazione d’impatto era, invece, dovuta, atteso che la valutazione d’impatto sulla protezione dei dati è sempre dovuta nel caso in cui il trattamento comporti “la sorveglianza sistematica su larga scala di una zona accessibile al pubblico” (v. art. 35, par. 3, lett. c), del Regolamento; cfr. le “Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video”, cit., par. 10)

L’obbligo di redigere una valutazione d’impatto era, peraltro, da considerarsi integrato anche ai sensi dell’art. 35, par. 1, del Regolamento, tenuto conto che risultavano sussistenti almeno tre dei criteri indicati dal Gruppo di lavoro art. 29 nelle “Linee guida in materia di valutazione d’impatto sulla protezione dei dati e determinazione della possibilità che il trattamento “possa presentare un rischio elevato” ai fini del regolamento (UE) 2016/679” del 4 aprile 2017, segnatamente il monitoraggio sistematico, il trattamento di dati aventi carattere altamente personale (relativi all’ubicazione), e il trattamento di dati su larga scala (v. sez. III).

Premesso che l’Autorità ha, pertanto, contestato alla Provincia la violazione dell’art. 35 del Regolamento, deve osservarsi che soltanto in sede di memoria difensiva l’Ente ha sostenuto che “la valutazione d’impatto è stata in realtà effettuata” e che “non è stata prodotta prima per una mera svista [...]”.

Nel rilevare che, limitatamente a tale profilo, la condotta tenuta dalla Provincia nei rapporti con l’Autorità non può ritenersi rispondente al canone della “responsabilizzazione” (art. 5, par. 2, del Regolamento), deve comunque osservarsi che la documentazione prodotta in atti (v. allegati alla nota del XX) consiste in due documenti, entrambi denominati “Valutazione di impatto sulla protezione dei dati relativi al sistema di rilevazione dei flussi di traffico veicolare sui passi dolomitici”, recanti meri riferimenti temporali (“XX” e “XX”) ma privi di data certa (ad esempio, mediante acquisizione al protocollo informatico dell’Ente). Tali documenti non rispondono poi, in ogni caso, ai requisiti sostanziali di cui all’art. 35 del Regolamento, non essendo stata effettuata una valutazione della probabilità e della gravità dei rischi derivanti in astratto dai trattamenti, dell’efficacia delle misure tecniche e organizzative prefigurate ai fini della mitigazione di tali rischi (cfr. art. 35, par. 7, lett. c) e d) del Regolamento) e del complessivo livello di rischio residuo all’esito delle predette misure (cfr. art. 36, par. 1, del Regolamento; cfr. le “Linee guida in materia di valutazione d’impatto sulla protezione dei dati e determinazione della possibilità che il

trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" del Gruppo di lavoro art. 29, adottate il 4 ottobre 2017 - WP 248 rev.01, fatte proprie dal Comitato europeo per la protezione dei dati con "Endorsement 1/2018" del 25 maggio 2018, ove si evidenzia che "ogniquale volta il titolare del trattamento non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare l'autorità di controllo"); v. anche l'"Allegato 2 - Criteri per una valutazione d'impatto sulla protezione dei dati accettabile" delle medesime Linee guida, ove si richiede che nella valutazione d'impatto vengano gestiti "i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c))", determinando "l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) [...] dalla prospettiva degli interessati; si considerano le fonti di rischio (considerando 90)", individuando "gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati", nonché "minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati", stimando "la probabilità e la gravità (considerando 90)", per poi determinare "le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90)").

Risulta, pertanto, confermato che la Provincia ha agito in violazione dell'art. 35 del Regolamento.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice, seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano insufficienti a consentire l'archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Si confermano, pertanto, le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato dalla Provincia, per aver trattato posto in essere un trattamento di dati personali, mediante dispositivi video, in violazione degli artt. 5, par. 1, lett. a) ed e), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 12, par. 1, 13, 21, par. 4, 26 e 35 del Regolamento, nonché 2-ter del Codice.

Tenuto conto che la violazione delle predette disposizioni ha avuto luogo in conseguenza di un'unica condotta (stesso trattamento o trattamenti tra loro collegati), trova applicazione l'art. 83, par. 3, del Regolamento, ai sensi del quale l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, le violazioni più gravi, relative agli artt. 5, 6, 12, 13 e 21 del Regolamento, nonché 2-ter del Codice, sono soggette alla sanzione prevista dall'art. 83, par. 5, del Regolamento, come richiamato anche dall'art. 166, comma 2, del Codice, l'importo totale della sanzione è da quantificarsi fino a euro 20.000.000.

5. Misure correttive (art. 58, par. 2, lett. d) e f), del Regolamento).

Tenuto conto che nella documentazione in atti vi è evidenza della sola disattivazione dei dispositivi video collocati nel territorio della Provincia di Trento, su espressa richiesta di quest'ultima (v. la nota della Provincia del XX, prot. n. XX, con cui si è data conferma di tale circostanza) e stante la rilevata illiceità del trattamento, si rende necessario ingiungere alla Provincia, ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, di cancellare senza ritardo i dati personali raccolti nell'ambito del progetto, nonché di imporre alla stessa, ai sensi dell'art. 58, par. 2, lett. f), del Regolamento, il divieto di ogni ulteriore trattamento mediante dispositivi video, installati sul territorio proprio o, in virtù di convenzioni o altri accordi contrattuali, su quello di altri soggetti pubblici e impiegati

nell'ambito del medesimo progetto.

Ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, la Provincia dovrà provvedere a comunicare a questa Autorità, fornendo un riscontro adeguatamente documentato, entro trenta giorni dalla notifica del presente provvedimento, le iniziative intraprese al fine di dare attuazione a quanto sopra ingiunto ai sensi del citato art. 58, par. 2, lett. d) e f), del Regolamento.

6. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i e 83 del Regolamento; art. 166, comma 7, del Codice).

Il Garante, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie la violazione delle disposizioni citate è soggetta all'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

Tenuto conto che:

ancorché la Provincia abbia conservato i dati relativi ai veicoli in transito per un esteso arco temporale, potendo così astrattamente ottenere informazioni delicate relative agli spostamenti di un numero elevato di interessati sul territorio osservato, la stessa non ha trattato gli stessi nell'ambito dei procedimenti amministrativi di propria competenza; l'Ente ha, dunque, agito con l'intento di servire un interesse pubblico, seppur, in maniera colposa, nell'erronea convinzione che sussistesse un idoneo quadro giuridico di settore a supporto dell'iniziativa intrapresa o che le informazioni raccolte non costituissero dati personali (art. 83, par. 2, lett. a) e b), del Regolamento);

la Provincia ha adottato misure per pseudonimizzare i dati oggetti di trattamento, così mitigando il rischio di identificazione degli interessati da parte di eventuali terzi (art. 83, par. 2, lett. a), del Regolamento);

i trattamenti posti in essere, pur potendo determinare un condizionamento della fruizione degli spazi pubblici da parte degli interessati, specialmente in assenza di un'adeguata informativa sul trattamento dei dati, non hanno causato conseguenze pregiudizievoli sulla sfera giuridica degli stessi, non essendo stati i dispositivi video impiegati per assumere decisioni nei loro confronti (art. 83, par. 2, lett. a), del Regolamento);

ancorché in maniera non adeguata, la Provincia aveva comunque apposto dei cartelli informativi in merito all'utilizzo di dispositivi video nelle aree interessate (art. 83, par. 2, lett. a), del Regolamento);

il trattamento non ha riguardato dati particolari appartenenti alle categorie particolari di cui all'art. 9 del Regolamento (cfr. art. 83, par. 2, lett. g), del Regolamento);

si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia medio (cfr. Comitato europeo per la protezione dei dati, "Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR" del 24 maggio 2023, punto 60).

Ciò premesso, nel considerare che il titolare del trattamento è un soggetto pubblico di rilevanza provinciale, si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze:

non risultano precedenti violazioni pertinenti commesse dalla Provincia in un medesimo contesto (art. 83, par. 2, lett. e), del Regolamento);

la Provincia ha offerto una buona cooperazione con l'Autorità nel corso dell'istruttoria (art. 83, par. 2, lett. f), del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 32.000 (trentaduemila) per la violazione degli artt. 5, par. 1, lett. a) ed e), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 12, par. 1, 13, 21, par. 4, 26 e 35 del Regolamento, nonché 2-ter del Codice, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò in considerazione del fatto che il trattamento ha riguardato i dati relativi ai veicoli in transito sul territorio interessato dal progetto, informazioni queste particolarmente delicate, atteso che, ancorché dall'istruttoria è emerso che la Provincia non abbia avviato alcun procedimento nei confronti di soggetti identificati mediante il numero di targa, dalla loro analisi possono essere astrattamente ottenute informazioni relative agli spostamenti degli interessati sul detto territorio, nonché tenuto conto che il trattamento ha avuto luogo per un esteso arco temporale.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO, IL GARANTE

dichiara, ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, l'illiceità del trattamento effettuato dalla Provincia Autonoma di Bolzano per violazione degli artt. 5, par. 1, lett. a) ed e), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 12, par. 1, 13, 21, par. 4, 26 e 35 del Regolamento, nonché 2-ter del Codice, nei termini di cui in motivazione;

ORDINA

alla Provincia Autonoma di Bolzano, in persona del legale rappresentante pro-tempore, con sede legale in Piazza Silvius Magnago 1 - 39100 Bolzano (BZ), C.F. 00390090215, di pagare la somma di euro 32.000 (trentaduemila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione. Si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

- alla predetta Provincia, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 32.000 (trentaduemila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento,

pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

- alla predetta Provincia, ai sensi dell'art. 58, par. 2, lett. d) ed f), del Regolamento, di cancellare senza ritardo i dati personali raccolti nell'ambito del progetto in questione, nonché imporre alla stessa il divieto di ogni ulteriore trattamento mediante dispositivi video, installati sul territorio proprio o, in virtù di convenzioni o altri accordi contrattuali, su quello di altri soggetti pubblici e impiegati nell'ambito del medesimo progetto, fornendo, altresì, al Garante, entro lo stesso termine, ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, un riscontro adeguatamente documentato in merito alle iniziative intraprese al fine di dare attuazione a quanto ordinato;

DISPONE

- ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione dell'ordinanza ingiunzione sul sito internet del Garante;

- ai sensi dell'art. 154-bis, comma 3 del Codice e dell'art. 37 del Regolamento del Garante n. 1/2019, la pubblicazione del presente provvedimento sul sito internet dell'Autorità;

- ai sensi dell'art. 17 del Regolamento del Garante n. 1/2019, l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2 del Regolamento, nel registro interno dell'Autorità previsto dall'art. 57, par. 1, lett. u) del Regolamento.

Ai sensi degli artt. 78 del Regolamento, 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 25 settembre 2025

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Fanizza