



Noemi Miniscalco

**UNO, NESSUNO O CENTOMILA?
MINIMIZZAZIONE E *PRIVACY*
BY DEFAULT NEL PRIMO
PROVVEDIMENTO DEL
GARANTE DOPO IL GDPR**

Estratto



GIUFFRÈ FRANCIS LEFEBVRE

**GARANTE PER LA
PROTEZIONE DEI DATI
PERSONALI**
28 GIUGNO 2018
N. 396
PRESIDENTE: SORO

RELATRICE: CALIFANO

PARTI: TESSERINI S.R.L. E
VISIRUN S.P.A.

**Dati personali • Regola-
mento Generale sulla Prote-
zione dei Dati Personali •
Localizzazione dei veicoli
aziendali • Valutazione di
impatto sulla protezione dei
dati personali • Principio di
minimizzazione • Privacy
by design e privacy by de-
fault**

I dati personali vanno tutelati fin

*dalla fase di progettazione di un
prodotto o di un servizio. Va per-
tanto ingiunto, ai sensi del Rego-
lamento Generale sulla Prote-
zione dei Dati Personali 679/
2016/UE a un fornitore di servizi
di geolocalizzazione, di incorpo-
rare il “diritto alla privacy” di-
rettamente nelle funzionalità del
prodotto, attenendosi al principio
di minimizzazione dei dati e a
quello di privacy by design e pri-
vacy by default.*

PREMESSO. — **1.1. La segnalazione nei confronti della società.** Un dipendente (all'epoca dei fatti segnalati) della Tesserini s.r.l. (di seguito, la società) ha lamentato con segnalazione che quest'ultima avrebbe effettuato il trattamento di dati personali a sé riferiti mediante l'installazione di un dispositivo GPS a bordo dell'autovettura aziendale, in assenza di una previa informativa o, comunque, della comunicazione di una policy aziendale relativa all'esistenza ed alle caratteristiche essenziali del sistema di geolocalizzazione. Tale sistema tecnologico avrebbe consentito al datore di lavoro la raccolta ed il successivo trattamento di dati relativi alla posizione geografica del dipendente anche al di fuori dell'orario di servizio, considerato che i veicoli aziendali sarebbero stati affidati con “autorizzazione all'utilizzo promiscuo”, senza obbligo di riconsegna del veicolo al termine della prestazione lavorativa.

1.2. La società, in risposta ad una prima richiesta di elementi formulata dall'Ufficio, ha dichiarato che:

a. nello svolgimento della propria attività, consistente nella “distribuzione e commercializzazione di impianti per saldatura e macchine per saldare” e della relativa assistenza ai clienti, ha installato su furgoni aziendali, “atteso l'elevato valore dei macchinari trasportati”, dispositivi di geolocalizzazione mediante sistema GPS (cfr. nota 27.7.2016, p. 1, lett. a);

b. i furgoni aziendali dotati di tali dispositivi, sui quali sono state apposte “vetrofanie conformi al provvedimento di carattere generale emesso dal Garante [...] rientrano ogni sera presso la sede di Rignano sull'Arno [...] pertanto nessun controllo tramite sistemi di localizzazione avviene al di fuori dell'orario di lavoro” (cfr. nota cit., p. 1, lett. a);

c. il sistema, oltre alla posizione geografica del veicolo, consente di trattare dati relativi ai “consumi di carburante, [ai] chilometri progressivi percorsi e la velocità media” (cfr. nota cit., p. 2, lett. b);

d. le finalità perseguite sono logistiche ed organizzative (possibilità di “effettuare un intervento di riparazione con il veicolo più vicino in zona [...], assicurare inoltre una più efficiente gestione del parco veicoli”) nonché volte a “garantire la sicurezza e l'incolumità dei lavoratori ed infine [a] prevenire e contrastare eventi criminosi ai danni dei beni aziendali” (cfr. nota cit., p. 2, lett. b);

e. il “sistema di localizzazione, completo del servizio di televigilanza H24, consente di ottenere elevati sconti in sede assicurativa” (cfr. nota cit., p. 2, lett. b);

f. con riferimento all’osservanza della disciplina in materia di controlli a distanza, “attesa la modifica normativa dell’art. 4 L. 300/1970 [...] in applicazione della disciplina sul c.d. « bilanciamento di interessi », è stato riconosciuto il trattamento di tali dati [...], senza richiedere il consenso dell’interessato, rendendosi sufficiente una informativa completa allo stesso lavoratore” (cfr. nota cit., p. 2, lett. b);

g. i dati trattati “sono automaticamente registrati sul server del fornitore del servizio e cancellati decorsi 365 giorni mediante sovrascrittura dei dati più recenti” (cfr. nota cit., p. 2, lett. c);

h. la società può “consultare in tempo reale le suddette informazioni tramite un’interfaccia web ad accesso riservato mediante l’inserimento di username e password” (cfr. nota cit., p. 3, lett. c);

i. il trattamento è “effettuato sia presso la sede della Tesserini s.r.l. tramite il Responsabile dei Servizi Generali e Organizzazione, in persona del legale rappresentante pro-tempore, sia presso il fornitore del sistema di localizzazione designato come « responsabile esterno » per le attività connesse alla sicurezza informatica e adempimenti di notifica ai sensi dell’art. 37 comma 1 lett. a)” del Codice (cfr. nota cit., p. 3, lett. d);

j. ai dipendenti interessati “è stata rilasciata ampia informativa ex art. 13 del D. lgs. 196/2003” (cfr. nota cit., p. 3, lett. e).

1.3. Con successive note di riscontro ad ulteriori richieste di chiarimenti, la società ha altresì dichiarato che:

a. “l’accesso ai dati di localizzazione dei furgoni aziendali non è effettuato in maniera costante e continuativa [...] bensì unicamente in occasione delle finalità logistiche e di organizzazione”; più precisamente “l’accesso ai dati di rilevazione GPS” è effettuato, in concreto, “una volta al mese circa” (cfr. nota ricevuta il 20.10.2016, p. 1 e 2);

b. “il sistema [...] è configurato in modo tale da registrare i dati sul server fino ai 365 giorni antecedenti. Tale opzione [...] non è in alcun modo modificabile dal fruitore finale del servizio” (cfr. nota cit., p. 2);

c. il soggetto designato responsabile esterno del trattamento è il fornitore del servizio di localizzazione, Visirun S.p.A., che “ha adempiuto agli obblighi di effettuare la notificazione al Garante”, fornendo in proposito alla società specifica attestazione (cfr. All. 1, nota 20.10.2016 cit., contenente copia di una email datata 14.10.2016 proveniente da Visirun con la quale dichiara “di aver assolto, tramite procedura formale [...], agli obblighi di legge per la protezione dei dati personali in relazione al trattamento di dati che indicano la posizione geografica [...], secondo l’art. 37 del D. lgs. 196/2003”);

d. “l’intervallo temporale con cui il sistema esegue la rilevazione della posizione geografica è pari a 120 secondi come da specifica del servizio di abbonamento Visirun Light” (cfr. nota ricevuta il 30.3.2017, p. 2);

e. quanto alle modalità di consultazione dei dati raccolti dal sistema, questo “riporta geograficamente la posizione Gps del furgone, nonché [...] il percorso effettuato dal medesimo lungo la mappa, con

l'indicazione dei chilometri percorsi e del relativo tempo impiegato con il calcolo [...] della velocità media" (cfr. nota cit., p. 2);

f. la società ha affidato al responsabile esterno Visirun S.p.A. compiti relativi alle modalità del trattamento e alle misure di sicurezza (cfr. nota cit., p. 1-2);

g. il dispositivo è allo stato installato su "5 furgoni aziendali [...]. Ad eccezione del furgone muletto e salvo diverse esigenze organizzative, gli altri quattro sono assegnati ciascuno ai medesimi dipendenti e di tale assegnazione non viene memorizzato alcun dato" (cfr. nota ricevuta il 24.10.2017, p. 1);

h. "i report del sistema non consentono di risalire all'identità del conducente, ma le informazioni ricavabili hanno un valore puramente statistico [e] hanno lo scopo di implementare la sicurezza dei lavoratori, verificare l'efficienza della programmazione [...], nonché individuare i mezzi maggiormente utilizzati per gestire con efficienza la rotazione degli stessi, al rafforzamento della flotta aziendale in caso di furto, nonché ai vantaggi economici relativi alla scontistica in sede assicurativa" (cfr. nota cit., p. 1-2).

1.4. Visirun S.p.A., fornitore del servizio di localizzazione utilizzato dalla società, rispondendo a due richieste di elementi da parte dell'Ufficio ha precisato che:

a. il contratto stipulato con Tesserini s.r.l. avente ad oggetto la fornitura del servizio di localizzazione satellitare di autovetture è stato sottoscritto in data 16.2.2012 ed è, allo stato, ancora in essere (nota ricevuta il 19.6.2017, p. 1);

b. il sistema fornito consente al cliente di effettuare la "verifica, in tempo reale, della posizione dell'autovettura aziendale"; la "verifica del percorso effettuato dall'autovettura [...] nell'arco della giornata"; nonché di esaminare la "reportistica di base della percorrenza chilometrica, tempi di guida, soste, etc." (cfr. nota cit., p. 2);

c. con riferimento alla tipologia dei dati trattati in occasione della fornitura del servizio "Visirun [...] non ha alcun interesse/intenzione a conoscere, in alcun momento, il nominativo della persona alla guida del veicolo aziendale" (cfr. nota cit., p. 2);

d. Tesserini s.r.l. ha designato Visirun S.p.A. quale responsabile esterno del trattamento, con un "documento [...] generico [...]"; inoltre Visirun "non ha mai ricevuto, da parte di Tesserini, ulteriori istruzioni e/o indicazioni relative al trattamento dei dati raccolti nell'erogazione del servizio, contrariamente a quanto dichiarato da Tesserini" (cfr. nota cit., p. 3);

e. "i dispositivi di localizzazione forniti [...], quando rilevano il movimento dell'autovettura su cui sono installati, iniziano ad acquisire automaticamente le coordinate geografiche e la velocità GPS del veicolo medesimo; la rilevazione delle coordinate avviene con intervalli di 60 secondi; i dispositivi inviano, ad intervalli predefiniti di 120 secondi, la posizione dell'autoveicolo aziendale al Centro Servizi Visirun"; il cliente può accedere ai dati raccolti e conservati presso il Centro servizi attraverso il sito web www.visirun.com, utilizzando le proprie credenziali di accesso (cfr. nota cit., p. 3);

f. i dati raccolti, relativi a ciascuna autovettura del cliente, “così come avviene per tutte le versioni « standard » del servizio — vengono cancellati da tutti i sistemi di Visirun, automaticamente, decorsi 365 giorni (1 anno) dal loro primo trattamento” (cfr. nota cit., p. 4);

g. “su richiesta espressa dei propri clienti, Visirun offre la possibilità ai medesimi di personalizzare alcune modalità del trattamento dei dati, tra cui: l’intervallo temporale con cui il sistema effettua la rilevazione della posizione geografica e i tempi di conservazione dei dati” (cfr. nota cit., p. 4);

h. Tesserini s.r.l. “non ha mai richiesto alcune di queste modifiche” (cfr. nota cit., p. 4);

i. Visirun ha effettuato “già nel 2009 (quale Mobivision s.r.l.) — la notificazione al Garante [...] ai sensi dell’articolo 37 del [Codice], successivamente aggiornata [...] a fronte delle intervenute modifiche societarie” posto che “nei confronti dei propri clienti, può affiancare al Servizio descritto [...], una serie di funzionalità ulteriori e differenti: è nell’erogazione di queste funzionalità ulteriori ([...] mai [...] richieste da Tesserini) che Visirun, sempre in qualità di « responsabile del trattamento » [...], potrebbe trattare dati personali dei propri clienti” (cfr. nota cit., p. 6);

j. attraverso la funzionalità “Comunicazione con l’operatore tramite l’invio di messaggi di testo”, indicata nel contratto di fornitura del servizio stipulato con Tesserini s.r.l., è possibile “inserire, in totale autonomia, [ulteriori] dati e informazioni, tra cui un « numero di telefono » [...] direttamente dal cliente” (cfr. nota ricevuta il 18.10.2017, p. 2).

1.5. All’esito di accertamenti ispettivi disposti dall’Autorità a fronte di circostanze non del tutto chiarite in atti (e di rappresentazioni contrastanti di fatti da parte del segnalante e della società), effettuati dal Nucleo speciale Privacy della Guardia di Finanza in data 14 e 15 febbraio 2018, è emerso che:

a. “Visirun ha fornito alla Tesserini sette dispositivi di geolocalizzazione, ma allo stato attuale sono installati e funzionanti solo cinque [...], montati esclusivamente sui furgoni aziendali” (cfr. verbale accertamenti ispettivi 14.2.2018, p. 3);

b. “non c’è un’associazione diretta e univoca dei furgoni ai dipendenti che li utilizzano; [...] non c’è alcun tipo di registro relativo all’organizzazione del servizio giornaliero, in quanto l’utilizzo dei furgoni da parte dei dipendenti avviene a seconda delle caratteristiche del servizio da svolgere” (cfr. verbale accertamenti ispettivi 15.2.2018, p. 2);

c. tra la documentazione consegnata nel corso dell’ispezione risulta: la dichiarazione di Visirun S.p.A., datata 14.2.2018, con la quale si rappresenta che Tesserini s.r.l. usufruisce del servizio di localizzazione “dal 2.10.2009 con abbonamento Light copertura nazionale per un totale di 7 localizzatori” (cfr. verbale 14.2.2018, All. 2); copia di autorizzazioni all’utilizzo di automezzo aziendale rilasciate da Tesserini s.r.l. in relazione a ciascun autoveicolo aziendale (sia furgoni che autovetture) con le quali si “autorizza” un elenco di dipendenti identificati (tra i quali il segnalante) “a condurre l’automezzo per esigenze connesse alla operatività aziendale e saltuariamente ed occasionalmente per esigenze di carattere personale”,

nonché “si riconosce [ai suddetti conducenti] facoltà degli stessi, limitatamente ed esclusivamente all'utilizzo non aziendale, di concederne l'uso a familiari conviventi, purché abilitati alla guida di autoveicoli nel territorio/nazione ove il medesimo viene utilizzato. Si precisa infine che l'utilizzo per scopi ed esigenze non aziendali del bene concesso in uso, viene regolato in osservanza delle norme fiscali vigenti” (a partire dal 27.8.2014 fino all'11.9.2017) (cfr. verbale 14 e 15.2.2018, All. 11 e 16);

d. “la Visirun ha fornito alla Tesserini sette dispositivi di geolocalizzazione, ma allo stato attuale sono installati e funzionanti solo cinque dispositivi [...]. Le due prime installazioni risalgono all'anno 2009 [...]” (cfr. verbale 14.2.2018, p. 3);

e. nel corso di verifiche dirette è stato accertato che su ciascun veicolo aziendale era stata apposta la vetrofanìa contenente l'informativa “minima” circa l'installazione del dispositivo di localizzazione (cfr. verbale 15.2.2018, p. 1).

1.6. Con nota pervenuta dopo l'effettuazione degli accertamenti in loco (in data 2.3.2018), la società ha infine dichiarato che:

a. con riferimento ai due dispositivi di geolocalizzazione tutt'ora oggetto di contratto di fornitura ma che non risulterebbero sui veicoli aziendali in uso, in un caso “con ogni probabilità” non si è provveduto “per mera dimenticanza” a smontare il dispositivo da un veicolo incidentato e destinato alla demolizione (cfr. nota cit., p. 1); in relazione al secondo dispositivo questo “non è stato rinvenuto e si presume che sia stato gettato come rifiuto”, in ogni caso “si esclude fermamente che il predetto dispositivo fosse presente sull'autovettura Mercedes” in uso al segnalante (cfr. nota cit., p. 2);

b. non sono state reperite le “informative del 2009” relative all'installazione di dispositivi di localizzazione geografica fornite agli interessati (cfr. nota cit., p. 2).

2. L'esito dell'istruttoria. All'esito dell'esame delle dichiarazioni rese all'Autorità nel corso del procedimento nonché della documentazione acquisita, emerge che Tesserini s.r.l., in qualità di titolare, effettua operazioni di trattamento di dati personali dei dipendenti mediante dispositivi di localizzazione geografica dei veicoli aziendali — forniti a partire dal 2 ottobre 2009 (v. precedente punto 1.5., lett. c.) da Visirun S.p.A., designata responsabile del trattamento — che risultano per alcuni profili non conformi alla disciplina in materia di protezione dei dati personali, nei termini di seguito descritti.

In proposito si ritiene preliminarmente che, contrariamente a quanto sostenuto dalla società, gli autisti alla guida dei veicoli aziendali sottoposti a localizzazione siano in concreto identificabili, considerato — quantomeno — il numero limitato dei veicoli stessi (allo stato, secondo quanto accertato, in numero di cinque, di cui uno con funzione di “muletto”), peraltro destinati ciascuno allo svolgimento di servizi determinati, nonché alla luce delle finalità dichiarate dalla società stessa, riconducibili proprio alla necessità di contattare gli autisti per effettuare con rapidità interventi in loco oppure per consentire l'efficiente gestione del parco veicoli e, infine, per garantire la sicurezza dei dipendenti stessi. Inoltre la società,

in caso di contestazioni di violazioni amministrative effettuate con modalità non immediata, è tenuta a ricondurre ad un autista determinato la relativa responsabilità.

3. Liceità, necessità, pertinenza e non eccedenza dei trattamenti effettuati. Gli scopi perseguiti dal titolare del trattamento con l'installazione del sistema soddisfano, secondo quanto rappresentato, la necessità di individuare rapidamente il veicolo più vicino in caso di richiesta di intervento nonché di gestire efficientemente il parco veicoli. Inoltre il sistema consentirebbe alla società di rafforzare la sicurezza dei dipendenti e dei beni aziendali, permettendo nel contempo di ottenere benefici in occasione della stipula di contratti di assicurazione dei veicoli aziendali (v. precedenti punti 1.2. lett. *d.* e *e.*).

In relazione a tali finalità è emerso che le concrete modalità di funzionamento del sistema tecnologico adottato consentono alla società, mediante il collegamento con la piattaforma web messa a disposizione dal fornitore del servizio, di visualizzare, attraverso la sezione "Mappa", in tempo reale la posizione dei veicoli acquisita dal sistema ogni 120 secondi, il loro stato (fermo/in movimento), la velocità nonché dati ulteriori relativi all'utilizzo del veicolo nella giornata in corso (le ore di impegno e di guida, le ore di pausa, la velocità media, indicate sia in totale che distintamente per ciascuna tratta effettuata, anche di pochi minuti). Tali informazioni sono rese disponibili, congiuntamente alla mappa geografica dei percorsi effettuati giornalmente, per un anno (365 giorni) (cfr. nota della società 30.3.2017 All. 3 e 4 e nota Visirun S.p.A. 19.6.2017, All. 4 "Descrizione del servizio erogato a Tesserini s.r.l."). L'ulteriore sezione "Report" consente all'utente del servizio di estrarre dati totali relativi all'utilizzo dei veicoli ("data", "veicolo", "ora inizio", "ora fine", "ore impegno", "ore percorrenza", "ore guida", "ore pausa", "ore riposo", "ore motore acceso", "Km", "Km di guida") ed anche "estrarre i dati, per ogni veicolo, relativi [...] agli ultimi 365 giorni, esportabili anche in formato excel o pdf" (cfr. nota Visirun S.p.A. 19.6.2017, All. 4 "Descrizione del servizio erogato a Tesserini s.r.l.", p. 2). È inoltre consultabile la sezione "Configurazioni", implementata dal cliente del servizio nonché la funzione "opzionale denominata « Privacy » che permette al conducente del veicolo, attraverso un interruttore che può essere installato (su scelta esclusiva del cliente) nel dispositivo presente nel veicolo, di disabilitare la tracciabilità del veicolo medesimo e quindi la memorizzazione dei relativi dati" (cfr. nota Visirun S.p.A. cit., All. 4, p. 2-3").

Tali modalità del trattamento e, segnatamente, la raccolta di informazioni particolareggiate sull'attività dei singoli veicoli monitorati dal sistema e, indirettamente, sull'attività degli autisti cui i veicoli sono affidati, quali la ricostruzione su mappa dei percorsi effettuati sia in tempo reale che giornalmente, con ulteriore distinta ricostruzione anche per ciascuna tratta dei percorsi effettuati e delle relative modalità, comprese le pause, con una periodicità della rilevazione estremamente ravvicinata (ogni 120 secondi), non sono proporzionate con gli scopi rappresentati dalla società (v. artt. 11, comma 1, lett. *d*) del Codice e 5, par. 1, lett. *c*) del Regolamento (UE) 2016/679) che potrebbero essere utilmente e legittimamente perseguiti con la raccolta di informazioni assai più limitate. Né

risulta conforme al principio di proporzionalità la integrale conservazione dei dati raccolti per un esteso periodo di tempo (365 giorni) in relazione alle finalità perseguite (v. artt. 11, comma 1, lett. e) del Codice e 5, par. 1, lett. e) del Regolamento (UE) 2016/679; per l'applicazione dei principi di necessità e proporzionalità in relazione a trattamenti di localizzazione di veicoli aziendali si veda anche quanto stabilito dal Garante in provv. 16.3.2017 n. 138, doc. web n. 6275314; provv. 30.11.2017 n. 505, doc. web n. 7522639 e provv. 24.5. 2017, doc. web n. 6495708).

Sotto il profilo della proporzionalità del trattamento effettuato, inoltre, si osserva che la società non ha — quantomeno — adottato il pur disponibile dispositivo di disattivazione della rilevazione geografica durante le pause consentite dell'attività lavorativa (c.d. funzione Privacy utilizzabile, secondo quanto dichiarato da Visirun S.p.A., anche per il tipo di servizio fornito a Tesserini s.r.l.).

Il sistema utilizzato è dunque in concreto idoneo a realizzare il monitoraggio continuo dell'attività del dipendente, in violazione dei principi di necessità, pertinenza e non eccedenza (in relazione agli artt. 3 e 11, comma 1, lett. d) e e) del Codice e 5, par. 1, lett. c) e e) del Regolamento (UE) 2016/679), considerato anche che il sistema medesimo è stato ed è utilizzato nella versione “standard”, in assenza di alcuna istruzione impartita al fornitore del servizio circa le caratteristiche essenziali dei trattamenti da effettuare (parametrabili in base alle concrete necessità dei clienti sia per quanto riguarda la periodizzazione temporale della rilevazione geografica che dei tempi di conservazione o attraverso la selezione delle funzionalità astrattamente disponibili; cfr. All. nota 24.10.2017 contenente copia della designazione del responsabile del trattamento).

In definitiva il titolare non ha provveduto a configurare il sistema tecnologico mediante misure adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (cfr. in proposito, oltre agli articoli sopra citati, anche l'art. 25 del Regolamento (UE) 2016/679, in attuazione del principio di c.d. privacy by default; si veda anche il Provvedimento di carattere generale in materia di localizzazione dei veicoli nell'ambito del rapporto di lavoro, 4 ottobre 2011, n. 370, in www.garanteprivacy.it, doc. web n. 1850581, laddove il Garante ha stabilito che “nel rispetto del principio di necessità (artt. 3 e 11, comma 1, lett. d), del Codice), la posizione del veicolo di regola non dovrebbe essere monitorata continuativamente dal titolare del trattamento, ma solo quando ciò si renda necessario per il conseguimento delle finalità legittimamente perseguite”).

4. L'informativa all'interessato. In relazione all'obbligo, posto in capo al titolare, di fornire prima dell'inizio dei trattamenti un'informativa ai dipendenti circa le caratteristiche essenziali degli stessi, come prescritto dall'articolo 13 del Codice (dal 25 maggio 2018 dall'articolo 13 del Regolamento (UE) 2016/679) e conformemente al principio di correttezza di cui all'art. 11, comma 1, lett. a) del Codice (dal 25 maggio 2018 anche dall'art. 5, par. 1, lett. a) del Regolamento (UE) 2016/679), mentre nel corso degli accertamenti ispettivi sono risultate apposte sui veicoli le vetrofanie a titolo di informativa “minima”, il titolare non ha fornito all'Autorità elementi idonei a documentare l'avvenuto adempimento del-

l'obbligo di fornire la dovuta informativa nei termini su esposti a far data dalla sottoscrizione del contratto con il fornitore del servizio di localizzazione (il 2.10.2009), limitandosi a fornire copia di un modello di informativa "in bianco", privo di data e di sottoscrizione (cfr. All. 1, nota 20.10.2016).

Pertanto i trattamenti effettuati risultano, anche sotto tale profilo, illeciti.

5. La disciplina lavoristica. La raccolta sistematica dei dati relativi alla posizione dei veicoli e la consultazione delle informazioni messe a disposizione attraverso l'accesso alla piattaforma web, sia in tempo reale sia attraverso elaborazioni e report conservati per un esteso periodo di tempo (365 giorni), consente alla società di effettuare il controllo dell'attività dei dipendenti.

Ciò risulta in contrasto con la disciplina di settore in materia di controlli a distanza (cfr. artt. 11, comma 1, lett. *a*) e 5, par. 1, lett. *a*) del Regolamento (UE) 2016/679 in relazione agli artt. 114 del Codice e 4, legge 20.5.1970, n. 300). Tale disciplina infatti, pure a seguito delle modifiche disposte con l'art. 23 del decreto legislativo 14 settembre 2015, n. 151, non consente l'effettuazione di attività idonee a realizzare il controllo massivo, prolungato e indiscriminato dell'attività del lavoratore (v. Provvedimento generale in materia di localizzazione dei veicoli aziendali cit., spec. par. 3; si vedano anche Article 29 Working Party, Opinion 2/2017 on data processing at work, WP 249, spec. n. 5.7. e Consiglio di Europa, Raccomandazione del 1 aprile 2015, CM/Rec (2015)5, spec. n. 16).

Con riferimento alla possibilità che la funzionalità di geolocalizzazione operi anche al di fuori dell'attività lavorativa o comunque del tempo di lavoro (ad es. durante le pause consentite dell'attività), si prende atto che in relazione al caso oggetto di segnalazione non è stato possibile accertare se la vettura in uso al segnalante fosse o meno sottoposta a geolocalizzazione attraverso il sistema. Ciò in quanto la società dichiara di non aver installato il dispositivo fornito di Gps su quel determinato autoveicolo (per quanto la società medesima non sia stata in grado di rintracciare due dispositivi tutt'ora oggetto di contratto di fornitura, v. precedente punto 1.6., lett. *a*.); mentre il segnalante ha dichiarato di aver appreso casualmente, dopo l'inizio del rapporto di lavoro, dell'operatività del dispositivo collegato al satellitare (si veda in proposito copia di una email, datata 1.2.2016, allegata alla segnalazione, nella quale uno dei titolari della società fa riferimento ad un "impianto satellitare" della cui esistenza il segnalante sarebbe stato informato "verbalmente").

Risultano in ogni caso in atti i documenti rilasciati dalla società in tempi diversi (il più recente datato 11.9.2017) agli autisti dei veicoli aziendali (anche quelli pacificamente sottoposti a geolocalizzazione) a titolo di "Autorizzazione all'utilizzo di veicolo aziendale", con i quali il rappresentante legale della società (che sottoscrive), con formula standard, autorizza l'utilizzo del mezzo — ancorché "saltuariamente ed occasionalmente" — "per esigenze di carattere personale". Si riconosce altresì la facoltà, "limitatamente ed esclusivamente all'utilizzo non aziendale", di "concederne l'uso a familiari conviventi, purché abilitati alla guida di autoveicoli" (cfr. precedente punto 1.5., lett. *c*.).

Pertanto la società (come frequentemente previsto in caso di utilizzo di veicoli aziendali) contempla l'utilizzo — seppur occasionale — di veicoli sottoposti al descritto sistema anche per esigenze di carattere personale. In tal modo l'operatività della funzionalità di geolocalizzazione (a maggior ragione se connotata dalle descritte caratteristiche di pervasività e frequenza ravvicinata della rilevazione), in assenza — per di più — della possibilità di disattivare il sistema, è idoneo a consentire il trattamento di dati “non rilevanti ai fini della valutazione dell'attitudine professionale” del dipendente, in violazione dell'articolo 8 della legge 20 maggio 1970, n. 300 (si veda sul punto Corte Cass., 19.9.2016, n. 18302 che con riferimento alla violazione del menzionato art. 8 ha ritenuto che “acquisire e conservare dati che contengono (o possono contenere) simili informazioni importa già l'integrazione della condotta vietata”), nonché incidentalmente anche di dati riferiti a terzi.

Anche sotto tale profilo il trattamento effettuato risulta illecito in relazione all'art. 113 del Codice, che richiama il menzionato art. 8, l. 300/1970.

6. Omessa notificazione al Garante. In relazione ai descritti trattamenti di localizzazione geografica la società ha altresì omissso di effettuare la notificazione al Garante, come dovuto fino alla data del 25 maggio 2018 ai sensi dell'articolo 37, comma 1, lett. a) del Codice. Tale obbligo, in base alla disciplina applicabile all'epoca dei fatti oggetto di accertamento, è posto dall'ordinamento a carico del titolare (che, in quanto tale, esercita un potere decisionale del tutto autonomo su finalità e modalità del trattamento), prima dell'inizio dei trattamenti. Nel caso di specie e a tale scopo, dunque, a nulla vale l'avvenuta notificazione effettuata in nome proprio dal fornitore del servizio, in data 17.2.2009.

7. Conclusioni: illiceità del trattamento. Per i suesposti motivi, considerato che il trattamento dei dati effettuato dalla società attraverso il descritto sistema di localizzazione dei veicoli aziendali oggetto di accertamento risulta illecito per violazione degli artt. 3, 11, comma 1, lett. a), d) ed e), 13, 37, 113 e 114 del Codice, si impone, ai sensi dell'art. 58, par. 2, lett. f), del Regolamento (UE) 2016/679, il divieto di ulteriore trattamento dei predetti dati.

Si rammenta che ai sensi dell'articolo 11, comma 2, del Codice i dati personali trattati in violazione della disciplina in materia di trattamento dei dati personali “non possono essere utilizzati”.

Qualora la società decida di utilizzare in futuro un sistema di localizzazione dei veicoli aziendali potrà farlo applicando i principi e le disposizioni del Codice e del Regolamento richiamate nel presente provvedimento, provvedendo altresì ad effettuare una valutazione di impatto sulla protezione dei dati (v. artt. 35 e 36 del Regolamento (UE) 2016/679).

8. Prescrizioni relative alla fornitura del servizio di localizzazione da parte di Visirun S.p.A.. Considerato che dall'attività istruttoria è emerso che la versione standard dei servizi forniti da Visirun S.p.A. comporta trattamenti di dati personali relativi alla posizione geografica accentuatamente dettagliati (anche per la periodizzazione temporale assai

ravvicinata: 30, 60 o 120 secondi) e conservati per un lungo periodo di tempo, tenuto altresì conto che tali servizi sono largamente utilizzati per la gestione di flotte aziendali (dunque nell'ambito di rapporti di lavoro), si ritiene necessario impartire al fornitore del servizio di localizzazione alcune misure a tutela dei diritti e delle libertà degli interessati.

In particolare si ingiunge ai sensi dell'art. 58, par. 2, lett. d), del Regolamento (UE) 2016/679, a Visirun S.p.A. di informare i propri clienti, indipendentemente da una richiesta in tal senso, della possibilità di modificare il sistema rispetto alla impostazione standard, selezionando le funzionalità disponibili e modificando i parametri principali in relazione alle finalità perseguite dal cliente/titolare del trattamento. Ciò in base al principio di liceità e correttezza dei trattamenti (v. art. 11, comma 1, lett. a) del Codice e art. 5, par. 1, lett. a) del Regolamento (UE) 2016/679). Tra le informazioni da rendere con evidenza ai clienti dei servizi vi è anche la possibilità di attivare la funzione Privacy (disattivazione del dispositivo), che deve essere resa disponibile in relazione a tutte le modalità di abbonamento ai servizi senza eccessivi costi aggiuntivi.

In ogni caso si ritiene necessario che — in base al principio di minimizzazione dei dati e di quello di privacy by design e by default espressamente richiamati, rispettivamente, dall'art. 5, par. 1, lett. c) e dall'art. 25 del Regolamento (UE) 2016/679 — la versione standard dei servizi offerti attraverso il sistema di localizzazione sia configurato con modalità proporzionate rispetto al diritto alla riservatezza degli interessati (considerato che tra questi i dipendenti costituiscono un numero rilevante), in particolare con riferimento alla periodizzazione temporale della rilevazione della posizione geografica, ai tempi di conservazione dei dati ed alla messa a disposizione e memorizzazione delle mappe dei percorsi effettuati. Si prescrive pertanto a Visirun S.p.A. di modificare l'impostazione standard in base ai principi sopra indicati.

Tali prescrizioni dovranno essere adempiute entro e non oltre il 30 settembre 2018.

9. Aspetti sanzionatori. L'Autorità si riserva di valutare, con autonomo procedimento, la sussistenza dei presupposti per la contestazione di violazioni amministrative nei confronti della società titolare del trattamento, in relazione all'omessa informativa agli interessati e all'omessa notificazione al Garante (v. artt. 13 e 37 del Codice; cfr. precedenti punti 4 e 6).

TUTTO CIÒ PREMESSO, IL GARANTE. — 1. ritenuto illecito, nei termini di cui in motivazione (punti 3, 4, 5 e 6), il trattamento effettuato da Tesserini s.r.l. attraverso il sistema di localizzazione di veicoli aziendali in violazione degli artt. 3, 11, comma 1, lett. a), d) ed e), 13, 37, 113 e 114 del Codice, ai sensi degli artt. 143, comma 1, lett. c) del Codice e 58, par. 2, lett. f), del Regolamento (UE) 2016/679, vieta l'ulteriore trattamento dei dati indicati in premessa;

2. ingiunge ai sensi dell'art. 58, par. 2, lett. d), del Regolamento (UE) 2016/679 a Visirun S.p.A., fornitrice del servizio di localizzazione dei veicoli, entro e non oltre il 30 settembre 2018, di:

— informare i propri clienti circa la possibilità di modificare il sistema rispetto alla impostazione standard conformemente alle finalità perseguite nonché circa la possibilità di attivare la funzione che consente la disattivazione del dispositivo, in relazione a tutte le modalità di abbonamento ai servizi senza eccessivi costi aggiuntivi;

— configurare — in base al principio di privacy by design e by default — la versione standard dei servizi offerti attraverso il sistema di localizzazione con modalità proporzionate rispetto al diritto alla riservatezza degli interessati, in particolare con riferimento alla periodizzazione temporale della rilevazione della posizione geografica, ai tempi di conservazione dei dati ed alla messa a disposizione delle mappe dei percorsi effettuati;

3. ai sensi dell'art. 58, par. 1, del Regolamento (UE) 2016/679, invita i destinatari del provvedimento, altresì, entro 30 giorni dalla data di ricezione presente provvedimento, a comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto vietato e prescritto nel presente provvedimento e di fornire comunque riscontro adeguatamente documentato. Si ricorda che il mancato riscontro alla richiesta ai sensi dell'art. 58 è punito con la sanzione amministrativa di cui all'art. 83, par. 5, lett. e), del Regolamento (UE) 2016/679.

Ai sensi degli artt. 152 del Codice e 78 del Regolamento (UE) 2016/67, nonché dell'10 del d.lg. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

**UNO, NESSUNO O
CENTOMILA?
MINIMIZZAZIONE E
PRIVACY BY DEFAULT NEL
PRIMO PROVVEDIMENTO
DEL GARANTE DOPO IL
GDPR**

1. IL CASO.

Con provvedimento n. 396 del 28 giugno 2018 il Garante *privacy* torna ad occuparsi del trattamento dei dati personali effettuato tramite sistemi di localizzazione. Per la prima volta, però, da un lato, la liceità del trattamento viene verificata anche al lume delle disposizioni del Regolamento (UE) 2016/679¹; dall'altro, l'Autorità di controllo italiana ingiunge ad un fornitore di servizi di localizzazione di

¹ Come noto, il 25 maggio 2018 ha trovato piena applicazione il Regolamento (UE) 2016/679. Prima di tale data, il trattamento dei dati personali effettuato tra-

mite sistemi di localizzazione era già stato oggetto di verifiche preliminari. Tra le altre: AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Verifica preliminare. Tratta-*

incorporare il diritto alla *privacy* — per impostazione predefinita — nelle funzionalità del prodotto, dando concreto significato al principio di *privacy by design*.

Il procedimento muove dalla segnalazione di un dipendente del(l'illecito) trattamento dei propri dati personali effettuato dal suo datore di lavoro (titolare del trattamento) tramite un dispositivo di geolocalizzazione, installato sull'autovettura aziendale assegnatagli con possibilità di uso promiscuo, « in assenza di una previa informativa o, comunque, della comunicazione di una *policy* aziendale »², nonché dal fornitore del sistema di localizzazione, specificamente designato responsabile esterno del trattamento.

Il titolare del trattamento, dopo aver confermato di avere installato sui mezzi aziendali dispositivi di geolocalizzazione mediante sistema GPS, asseriva di avere fornito specifica informativa ai dipendenti e di non effettuare accessi ai dati di localizzazione in maniera costante e continuativa, tanto meno fuori dall'orario di lavoro, nonché di non poter in alcun modo risalire all'identità del conducente di ogni singolo veicolo aziendale.

Il trattamento — come ricostruito all'esito degli accertamenti ispettivi e dell'istruttoria procedimentale dall'Autorità — consisteva nella raccolta, registrazione e consultazione, mediante il collegamento con la piattaforma *web* messa a disposizione dal fornitore del servizio, dei dati relativi « [al]la posizione dei veicoli acquisita dal sistema ogni 120 secondi, [a]l loro stato (fermo/in movimento), [al]la velocità, nonché dati ulteriori relativi all'utilizzo del veicolo nella giornata in corso (le ore di impiego e di guida, le ore di pausa, la velocità media, indicate sia in totale che distintamente per ciascuna tratta effettuata, anche di pochi minuti) » e nella conservazione degli stessi per un periodo di 365 giorni³.

Il trattamento dei dati *de quibus* era posto in essere al fine di gestire le richieste di intervento, di garantire un efficiente utilizzo del parco veicoli, di sicurezza dei lavoratori e dei beni aziendali, per ottenere benefici in occasione della stipula di contratti di assicurazione, nonché, in caso di contestazioni di violazioni amministrative, « per ricondurre ad un autista determinato la relativa responsabilità »⁴.

Infine, non risultava essere stata implementata la funzione opzionale "Privacy", consistente in un interruttore che, una volta installato nel dispositivo di localizzazione, avrebbe permesso di disabilitare la traccia-

mento dei dati personali mediante un sistema di localizzazione geografica dei dispositivi aziendali, doc. web n. 9358266; Verifica preliminare. Trattamento dei dati personali derivanti dalla rilevazione di coordinate satellitari relative alla geolocalizzazione di apparati elettronici di tipo radio mobili e veicolari, doc. web n. 6495708; Verifica preliminare. Trattamento di dati personali di dipendenti effettuato attraverso la localizzazione di dispositivi *smartphone* e *tablet*, doc. web n. 7522639; Verifica preliminare. Trattamento di dati personali di dipendenti effettuato attraverso la localizzazione di veicoli aziendali, doc. web n. 6275314; nonché di un provve-

dimento generale: Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro, doc. web n. 1850581. Tutti i provvedimenti *de quibus* sono reperibili in www.garanteprivacy.it.

² Così si esprime l'Autorità garante per la protezione dei dati personali, punto 1.1 del provvedimento ivi in commento.

³ Punto 3 del provvedimento.

⁴ Finalità così ricostruite dall'Autorità nel punto 2 del provvedimento. L'affermazione è di particolare importanza perché anticipa le conclusioni del Garante quanto all'illiceità del trattamento anche per violazione della disciplina giuslavoristica, *sub specie* di divieto di controllo a distanza del lavoratore.

bilità e la memorizzazione, con conseguente minimizzazione dei dati raccolti.

All'esito della ricostruzione operata, il Garante per la protezione dei dati personali, ritenuto il trattamento illecito — poiché posto in essere in violazione degli articoli 3 e 11, comma 1, lett. a), d) ed e) del Codice in materia di protezione dei dati personali e dell'art. 5, par. 1, lett. c) ed e) del Regolamento (UE) 2016/679, del principio di *privacy by default*, di cui all'art. 25 del Regolamento, nonché degli articoli 13 del Codice e del Regolamento in relazione all'omessa informativa ai dipendenti in materia di protezione dei dati personali⁵, dell'art. 37 del Codice, in relazione all'omessa notificazione del trattamento⁶, e degli articoli 113 e 114 del Codice⁷ — ne ha vietato la prosecuzione.

Ai nostri fini, il provvedimento merita particolare attenzione nella parte relativa allo scrutinio della violazione dei principi di minimizzazione e di *privacy by default* da leggere in combinazione anche con le disposizioni del Codice in materia di protezione dei dati personali. In particolare, la preliminare ricostruzione dell'assetto normativo induce ad interrogarsi su quale sia la tecnica cui debba ricorrere l'interprete (*in primis*, il titolare del trattamento) per correttamente selezionare i soli dati pertinenti, adeguati e limitati a quanto necessario per il raggiungimento della finalità perseguita⁸. Tale questione, che per linearità verrà affrontata per ultima, non oscura la rilevanza del provvedimento anche sotto due ulteriori profili, che verranno esaminati nei prossimi due paragrafi: l'Autorità, da un lato, chiarisce la doverosità, nella vicenda oggetto di scrutinio e in casi analoghi, dell'esecuzione, prima dell'inizio del trattamento, di una valutazione di impatto *privacy*; dall'altro, facendo applicazione dei principi di *privacy by design* e *by default*, si sofferma sul ruolo dei fornitori di servizi nella predisposizione di sistemi *privacy oriented*⁹.

⁵ In particolare, la società, pur avendo sostenuto di aver adempiuto all'obbligo *de quo*, non aveva allegato elementi idonei a fornire in concreto la prova dell'adempimento. Per vero, è dovere del titolare del trattamento non soltanto adempiere, ma altresì dare prova dell'adempimento stesso.

⁶ Trattasi di obbligo che, fino al 25 maggio 2018, doveva essere adempiuto dal titolare prima dell'inizio del trattamento.

⁷ In particolare, il Garante ha ritenuto illecito il trattamento, per violazione degli artt. 113 e 114 del d. lgs. n.196 del 2003, conformandosi al suo precedente e consolidato orientamento (si veda per un approfondimento la nota n.1 del presente commento). Secondo l'Autorità di controllo, il datore di lavoro era in concreto in grado di identificare — sia per il numero limitato di mezzi di trasporto, utilizzati ciascuno per precisi servizi, sia in considerazione delle finalità perseguite dalla società

— i dipendenti che, nell'espletamento delle proprie mansioni, utilizzavano i veicoli soggetti a localizzazione, con conseguente violazione del divieto di controllo a distanza dell'attività dei lavoratori. Sotto altro profilo, l'impossibilità di disattivare il sistema di geolocalizzazione comportava il trattamento di dati non rilevanti ai fini della valutazione dell'attitudine professionale del dipendente, in violazione dell'articolo 8 della legge n. 300/1970.

⁸ Si veda *infra* per l'approfondimento dei rapporti tra l'art. 5, par. 1, lett. c) del Regolamento e l'art. 11, lett. d), del Codice della *privacy*.

⁹ Per vero, ritenendo alto il rischio per i diritti e le libertà degli interessati, non ultimo per la mancata implementazione della funzione di disattivazione, essa ha ingiunto al responsabile esterno del trattamento (fornitore del servizio di localizzazione) di configurare, in ossequio ai principi di *privacy by design* e *by default*, i servizi offerti.

2. TRA RISCHIO E PERICOLO: UN CASO “CERTO” IN CUI È OBBLIGATORIO PROCEDERE ALLA VALUTAZIONE DI IMPATTO.

En passant, nelle conclusioni del provvedimento, il Garante per la protezione dei dati personali ha affermato che « qualora la società decida di utilizzare in futuro un sistema di localizzazione dei veicoli aziendali potrà farlo applicando i principi e le disposizioni del Codice e del Regolamento [...], provvedendo altresì ad effettuare una valutazione di impatto sulla protezione dei dati »¹⁰.

L'Autorità di controllo fa, dunque, luce sull'obbligatorietà della valutazione di impatto *privacy* in ipotesi di trattamenti effettuati tramite sistemi di localizzazione dei veicoli aziendali.

In particolare, la DPIA (*Data Protection Impact Assessment*) è « un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche »¹¹. Essa deve essere effettuata *obbligatoriamente* ogniquale volta il trattamento possa presentare un rischio elevato per le libertà e i diritti delle persone fisiche¹² ed è strumento di *responsabilizzazione* del titolare del trattamento, esplicitazione dell'approccio basato sul rischio adottato dal Regolamento. Come noto, infatti, con il GDPR si passa da un'analisi “statica” dei rischi, basata sull'adozione delle misure minime di sicurezza, ad una valutazione “dinamica”, atta a favorire un comportamento proattivo del titolare del trattamento che — alla luce del contesto, della natura, dell'oggetto e delle finalità dello stesso — deve scegliere tra le misure quelle più adeguate a mitigare il rischio¹³.

Ebbene, se proprio la valutazione di impatto è — fra le altre misure e procedure — quella che più di tutte (ri)porta al centro del sistema l'interessato, con i suoi diritti e libertà, concretizzando il passaggio dalla centralità del dato alla centralità della persona¹⁴, problematica è però l'individuazione dei casi in cui è obbligatorio effettuare una DPIA. Invero, l'articolo 35, par. 3 del Regolamento enuclea alcune ipotesi di trattamenti che, comportando, secondo una valutazione presuntiva, rischi elevati per i diritti e le libertà degli interessati, esigono l'esperimento

¹⁰ Cfr. punto 7 del provvedimento. Come noto, la valutazione di impatto sulla protezione dei dati personali, adempimento introdotto dal GDPR (art. 35), sostituisce il vecchio obbligo di cui all'art. 37 d. lgs. n.196 del 2003 posto a carico del titolare del trattamento.

¹¹ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *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*, adottate il 4 aprile 2017, 3, in <http://ec.europa.eu>.

Il Regolamento (UE) 2016/679 non dà una definizione di DPIA, ma ne descrive, all'art. 35, par. 7, il contenuto minimo. Si veda altresì al riguardo il Considerando n. 84.

¹² Articolo 35, par. 1 Regolamento (UE) 2016/679.

¹³ Per un approfondimento, si veda F. DI RESTA, *La nuova “Privacy europea”. I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Torino 2018, 124; F. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in ID. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino 2018, 63-73.

¹⁴ In particolare, la DPIA persegue due finalità: « garantire il rispetto dei capisaldi cardini della normativa, requisiti di *compliance* che sono indipendenti dal contesto nel quale si sviluppano i rischi » e « valutare l'impatto degli stessi sui diritti delle persone interessate » così F. DI RESTA, *La nuova “Privacy europea”*, cit., 127.

di una preventiva valutazione di impatto¹⁵: trattasi però di elencazione meramente esemplificativa e non esaustiva, come si evince dall'espressione « in particolare » di cui alla lettera della norma.

Per tale ragione, « al fine di fornire un insieme più concreto di trattamenti che richiedono una valutazione di impatto sulla protezione dei dati in virtù del loro rischio elevato intrinseco »¹⁶ il Gruppo Articolo 29 ha individuato, nelle linee guida in materia di valutazione di impatto, nove criteri che si pongono quale valido ausilio per l'interprete: se il titolare ritiene che il trattamento sia tale da integrare almeno due dei nove criteri enucleati, allora dovrebbe concludere per la doverosità di una DPIA¹⁷.

Tale schema logico, che pare dirimere ogni dubbio, è però infranto nelle stesse linee guida allorché viene chiarito che « tuttavia, in alcuni casi, [...] il titolare del trattamento (potrebbe) ritenere che un trattamento che soddisfi soltanto un [...] criterio richieda una valutazione di impatto sulla protezione dei dati »¹⁸ o, al contrario, che un trattamento che integri anche più criteri elaborati dal WP29 non sia tale da presentare un rischio elevato e quindi richiedere una DPIA.

Peraltro, da ultimo, il Garante *privacy* ha recentemente adottato l'elenco « delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati » ai sensi dell'art. 35, comma 4, del Regolamento (UE) 2016/679, nel quale compaiono, tra gli altri, i « trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti »¹⁹. L'emanazione dell'elenco *de quo*, confermando la ricostruzione operata dall'Autorità nel provvedimento ivi in commento, porta ora ad annoverare il trattamento effettuato tramite sistemi di localizzazione dei veicoli aziendali tra quelli in cui è « certa » la sussistenza di un rischio elevato per i diritti e le libertà degli interessati e — conseguentemente — necessaria una valutazione di impatto *privacy*²⁰.

¹⁵ Ai sensi dell'art. 35, par. 3 Reg. (UE) 679/2016: « La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico ».

¹⁶ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida*, cit., 8, in <http://ec.europa.eu>.

¹⁷ Più in generale, « maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione di impatto sulla protezione dei dati » (cfr. *Ivi*, 10).

¹⁸ *Ibidem*.

¹⁹ AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679*, doc. web n. 9058979, pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018.

²⁰ Pur essendo previsto (all'art. 35 GDPR) che occorre procedere ad una DPIA quando « il trattamento prevede l'uso di nuove tecnologie » e « considerata la na-

3. FORNITORE E UTILIZZATORE: LA MINIMIZZAZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA.

Venendo, ora, al secondo profilo poc'anzi evidenziato, il Garante, non solo ha vietato alla società la continuazione del trattamento (in quanto illecito)²¹ ma, in ottica di effettività della tutela dei diritti degli interessati, ha altresì prescritto al fornitore del servizio (responsabile esterno del trattamento), da un lato, di « configurare — in base al principio di *privacy by design e by default* — la versione *standard* dei servizi offerti attraverso il sistema di localizzazione con modalità proporzionate rispetto al diritto alla riservatezza degli interessati, in particolare con riferimento alla periodizzazione temporale della rilevazione della posizione geografica, ai tempi di conservazione dei dati ed alla messa a disposizione delle mappe dei percorsi effettuati »²²; dall'altro, di informare i propri clienti della possibilità di modificare il sistema rispetto alla impostazione *standard* e — più pregnantemente — di rendere disponibile in relazione a tutte le modalità di abbonamento la funzione che consenta la disattivazione del dispositivo di localizzazione « senza eccessivi costi aggiuntivi »²³.

L'Autorità ha, in altri termini, dato attuazione ai principi di *privacy by design* e *privacy by default* che prescrivono, l'uno, la necessità di tutelare i dati sin dalla fase di progettazione, l'altro, la tutela della vita privata per impostazione predefinita²⁴. Invero, ai sensi dell'art. 25 del Regolamento, il titolare del trattamento « sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso [...] mette in atto misure tecniche e organizzative adeguate [...] volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione »;

tura, l'oggetto, il contesto e le finalità del trattamento, esso può presentare un rischio elevato per i diritti e le libertà della persona fisica », non poteva infatti dirsi di per sé doverosa una valutazione di impatto del trattamento effettuato tramite sistema di localizzazione. Per vero, in assenza di un elenco, enucleato dal Garante, delle tipologie di trattamento per le quali sussista un obbligo di DPIA, la scelta di effettuare o meno la valutazione *de qua* restava pur sempre in capo al singolo titolare del trattamento, in ossequio al principio di *accountability*.

²¹ Secondo l'Autorità di controllo « la raccolta di informazioni particolareggiate sull'attività dei singoli veicoli monitorati dal sistema e, indirettamente, sull'attività degli autisti » era sproporzionata rispetto alle finalità perseguite (cfr. punto 3 del provvedimento). Conseguentemente, la violazione del principio di minimizzazione, che deve orientare il titolare del trattamento nella selezione dei soli dati pertinenti, adeguati e limitati a quanto necessario per il raggiungimento della finalità, determina l'illiceità del trattamento.

²² Cfr. il dispositivo del provvedimento ivi in commento. In egual modo, nel punto 3 del provvedimento si legge che « in definitiva il titolare non ha provveduto a configurare il sistema tecnologico mediante misure adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento [...] in attuazione del principio di c.d. *privacy by default* ».

²³ *Ibidem*.

²⁴ Sin dalla progettazione del processo di trattamento — *by design*, appunto — occorre attribuire importanza primaria alla protezione dei dati personali e vagliare ogni ipotesi alternativa che permetta una riduzione del rischio di verifica di eventi che possano pregiudicare i diritti e le libertà degli interessati. Al fondo, attraverso valutazioni sulla prevedibilità ed evitabilità dell'evento si *previene* la verifica di quest'ultimo (attraverso *in primis* la predisposizione di misure di sicurezza). Per un approfondimento, si veda, tra gli altri, L. GRECO, *I ruoli: Titolare e Responsabile*, in G. FINOCCHIARO, (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna 2017, 254 ss.

inoltre, « il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento ».

Ebbene, in ossequio al principio di *privacy by default* il titolare del trattamento deve adottare misure tecniche e organizzative che garantiscano, per impostazione predefinita, il diritto alla *privacy*, anche incorporandolo negli strumenti utilizzati; in tal modo, *automaticamente*, il trattamento avrà ad oggetto i soli dati *necessari*.

Se così è, la *privacy by default*, operando in una fase che precede l'inizio del trattamento stesso, non può che finire per incidere anche sulla progettazione degli strumenti e/o applicativi tramite i quali il trattamento può essere effettuato ²⁵.

Del resto, colui che costruisce il sistema, prima ancora dell'utilizzatore, svolge una funzione di determinazione dell'intero processo di trattamento e — in ultima analisi — delle scelte dell'utente. A conferma di ciò, il Considerando n. 78 del Regolamento (UE) 2016/679 chiarisce che « in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tener conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni ». Infatti, la selezione *by default* dei soli dati necessari — da “progettare” in un momento antecedente al trattamento — incide non solo sulla quantità dei dati raccolti, ma anche sulla portata del trattamento stesso, nonché sull'accessibilità e periodo di conservazione dei dati (c.d. principio della limitazione della conservazione).

A parere di chi scrive nell'ottica dell'effettività della tutela degli interessati, possono apprezzarsi le conclusioni del Garante per la protezione dei dati personali e le prescrizioni dallo stesso rivolte al responsabile esterno del trattamento; per vero, soprattutto l'ordine di rendere disponibile la funzione di disattivazione del dispositivo di localizzazione per ogni tipo di abbonamento offerto risulta essere misura adeguata sia sotto il profilo giuslavoristico ²⁶ (quale strumento idoneo ad impedire il con-

²⁵ Come è stato rilevato, la norma di cui all'art. 25 del Regolamento « può essere definita: a) ad effetto “immediato” perché riguarda addirittura la fase precedente all'avvio del trattamento; b) ad effetto “indiretto” perché si riflette anche sui fornitori di beni e servizi; c) a “testata multipla” perché può riguardare un numero molto ampio di soggetti, in ragione di quanti sono i produttori di beni o i fornitori di servizi di cui il titolare si avvale » (cfr. F. PIZZETTI, *La protezione dei dati personali e la sfida della Intelligenza Artificiale*, in *Ib.* (a cura di), *Intelligenza artificiale*, cit., 114).

²⁶ Si consideri inoltre che dalla qualificazione — non pacifica — dei sistemi di

localizzazione come strumenti utilizzati dal lavoratore per rendere la prestazione discende o meno l'applicazione della disciplina di maggior tutela di cui al comma 1 dell'art. 4 St. lav. (come da ultimo modificato dal d. lgs. n. 151 del 2015). Esclude la riconduzione degli strumenti *de quibus* nel *genus* “strumenti di lavoro” il MINISTERO DEL LAVORO E DELLE POLITICHE SOCIALI, *Controlli a distanza: Ministero del lavoro, nessuna liberalizzazione; norma in linea con le indicazioni del Garante della Privacy - Comunicato stampa*, 18 giugno 2015. Diversamente, L'ISPettorato Nazionale del Lavoro, con Circolare n. 2 del 7 novembre 2016, pur affermando che i GPS in linea di massima

trollo costante e anelastico dell'attività dei lavoratori), che di minimizzazione dei dati trattati.

Non può però sottacersi come, invece, in assenza di disposizioni (foss'anche di regolazione "leggera") che stabiliscano l'imprescindibilità del pulsante di disattivazione, in ottica *de jure condendo* ben auspicabili²⁷, l'imposizione della vendita di una specifica funzione del prodotto sul mercato « senza eccessivi costi aggiuntivi²⁸ » sembra contrastare con la libertà di impresa. In attuazione del provvedimento, infatti, il responsabile esterno del trattamento, per rendere fruibile la funzionalità per qualsiasi tipologia di abbonamento, potrebbe implementare il sistema o senza alcun costo aggiuntivo, oppure, più plausibilmente, traslandone il costo sul cliente. In quest'ultimo caso, tuttavia, egli, a fronte dell'ulteriore servizio reso disponibile, non potrebbe determinare liberamente il prezzo, dovendo rispettare il limite — indeterminato — di "non eccessività" imposto dal Garante, capace di incidere negativamente non soltanto sull'esplicazione della libertà d'iniziativa economica della singola impresa, ma — in ottica grandangolare — sulla posizione dell'operatore economico nel mercato di riferimento. Ebbene, in ragione dell'efficacia meramente *inter partes* del provvedimento del Garante, verrebbe a crearsi una situazione di potenziale svantaggio competitivo ai danni del destinatario del provvedimento richiamato, che non potrà traslare sul cliente l'intero costo del servizio aggiuntivo, se eccessivo; ciò a differenza di un concorrente, il quale, non essendo gravato dal medesimo vincolo, ben potrebbe rendere disponibile il medesimo servizio al costo ritenuto più congruente con la propria strategia di mercato.

4. IL PRINCIPIO DI MINIMIZZAZIONE, CHI ERA COSTUI?

Il Garante per la protezione dei dati personali, ritenuto illecito il trattamento effettuato dalla società tramite il sistema di localizzazione, poiché « in concreto idoneo a realizzare il monitoraggio continuo dell'attività del dipendente, in violazione dei principi di necessità, pertinenza e

sono un elemento aggiuntivo agli strumenti di lavoro, non essendo utilizzati in via primaria per l'esecuzione della prestazione ma, piuttosto, rispondendo ad esigenze ulteriori, non esclude la possibilità che il concreto utilizzo dei sistemi *de quibus* potrebbe portare a ritenere che in singoli casi essi debbano essere sussunti nella fattispecie di cui al comma 2 dell'art. 4 St. lav. In egual modo, parte della dottrina sottolinea come non sussista in astratto alcuna differenza ontologica tra gli strumenti di cui al primo o al secondo comma dell'art. 4 St. lav.; piuttosto, la loro qualificazione dipende dal nesso esistente tra gli strumenti stessi e lo svolgimento della prestazione (cfr. R. DEL PUNTA, *La nuova disciplina dei controlli a distanza sul lavoro* (art. 23 d.lgs. n. 151/2015), in *Riv. It. dir. lav.*, 2016, I, spec. 101; A. MARESCA, *Controlli tecnologici e tutele del lavoro nel nuovo art. 4 St. lav.*, in P.

TULLINI (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino 2017, 15).

²⁷ In tal modo, tramite la predisposizione della funzione di disattivazione, si assicurerebbe agli interessati (*id est* ai lavoratori) una maggior tutela della propria posizione soggettiva che — in ottica prospettica — potrebbe forse finanche qualificarsi come diritto "à la désactivation". L'espressione richiama volutamente "le droit à la déconnexion" di cui alla *Loi travail* francese dell'8 agosto 2016. Si veda, in ottica comparata, l'articolo 6 della Deliberazione n. 2015-165, del 4 giugno 2015, della COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS che, pur essendo attualmente privo di forza vincolante, rimane punto di riferimento per l'interpretazione e applicazione delle norme del GDPR.

²⁸ V. dispositivo del provvedimento ivi in commento.

non eccedenza (in relazione agli artt. 3 e 11, comma 1 lett. *d*) ed *e*) del Codice e 5, par. 1, lett. *c*) ed *e*) del Regolamento (UE) 2016/679) »²⁹, ne ha vietato la prosecuzione.

Il provvedimento — in parte *qua* — per un verso assume particolare rilievo alla luce dell'applicazione congiunta della disciplina nazionale e sovranazionale³⁰, che rende necessaria, *in primis*, una ricostruzione, in ottica sistemica, delle disposizioni violate, al fine di vagliarne eventuali sovrapposizioni in via diretta (ossia per coincidenza di formulazione letterale) ovvero indiretta (per il tramite dell'interpretazione, anche conforme); per altro verso esso impone all'interprete di interrogarsi su quale sia lo strumento per selezionare, per ogni singolo trattamento, i soli dati necessari per il raggiungimento della finalità perseguita (o, al contrario, scongiurare il rischio di porre in essere trattamenti di dati per scopi che ben avrebbero potuto essere « utilmente e legittimamente perseguiti con la raccolta di informazioni assai più limitate »³¹). Esaminiamo, partitamente, i due profili in questo e nel paragrafo successivo.

L'Autorità ha rilevato — correttamente — la violazione del principio di minimizzazione, vettore che deve indirizzare ogni titolare del trattamento nella scelta selettiva di quali informazioni riguardanti una persona fisica identificata o identificabile abbia *necessità* di acquisire per il raggiungimento delle sue finalità. La *ratio* del principio *de quo* ben si comprende se si muove dall'assunto per cui tra la quantità di dati personali trattati e il livello di rischio per i diritti e le libertà degli interessati sussiste un rapporto di proporzionalità diretta; infatti, all'aumentare della prima variabile, aumenterà necessariamente anche la seconda.

Già sotto la vigenza del “vecchio” Codice, il legislatore all'articolo 11, comma 1, lett. *d*) aveva sancito che i dati personali oggetto di trattamento dovevano essere « pertinenti, completi e non eccedenti rispetto alle finalità » perseguite.

Con il Regolamento è stato compiuto un passo in avanti: ai sensi dell'art. 5, par. 1, lett. *e*) i dati personali devono essere « adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati »; è questo — *stricto sensu* — il principio di minimizzazione dei dati.

Propriamente, tra le due disposizioni summenzionate non sussiste una relazione di identità; piuttosto, già dalla mera formulazione letterale, ben può cogliersi che, ferma restando la costante del requisito di *pertinenza* dei dati, il costruito cui è ricorso il legislatore è già esso espressione di un diverso approccio al dato personale e al grado di tutela che occorre ad esso assicurare.

Infatti, laddove il Codice richiede che il dato debba essere *completo*, il Regolamento — seguendo una logica “minimalista” — dispone che esso debba essere *adeguato*. Adeguatezza e completezza, lungi dall'essere concetti coincidenti, potrebbero porsi quali connotati contrastanti: un

²⁹ Cfr. punto n. 3 del provvedimento.

³⁰ Trattasi di discipline entrambe vigenti al momento dell'emanazione del provvedimento. Gli artt. 3 e 11 del Codice sono stati solo successivamente abrogati ad opera

del d. lgs. n.101 del 2018, nel più ampio disegno di adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679.

³¹ V. punto 3 del provvedimento.

dato potrebbe essere adeguato rispetto ad una determinata finalità, anche se non completo; oppure completo, ma non adeguato.

Focale è, però, il rilievo che assume la diversa formulazione della norma nella parte in cui sancisce che i dati devono essere non eccedenti rispetto alla finalità ovvero, secondo il disposto di cui al Regolamento, limitati a quanto necessario rispetto alla finalità. Ben può cogliersi il cambio di approccio determinato da una delimitazione — in negativo prima, in positivo poi — della quantità di dati che, al ricorrere degli altri presupposti, il titolare potrebbe lecitamente trattare. Per vero, la valenza semantica della non eccedenza implica la definizione di una soglia non superabile; quella della limitazione alla quantità necessaria richiede un presumibile abbassamento di tale soglia: non sarebbe possibile trattare quei dati che risultino essere — si badi bene, non tanto “eccedenti”, ma — non “limitati a quanto necessario” rispetto alla finalità perseguita.

Ebbene, nel nuovo assetto regolamentare, il principio di minimizzazione veicola le scelte non più solo individuando criteri di selezione dei dati per ogni singola operazione o suo segmento, secondo un approccio statico e *uno actu*, ma, più pregnantemente, divenendo metro per una tutela dinamica del diritto alla protezione dei dati personali³². Tutela che peraltro parte della dottrina aveva, già in passato, così ricostruito, interpretando estensivamente l’articolo 3 del d. lgs. 196/2003 (il c.d. principio di necessità), come riferito non soltanto ai meri sistemi informatici, ma piuttosto a qualunque strumento e/o procedura, anche non informatizzata³³.

Conseguentemente, il principio di minimizzazione, trovando attuazione in qualunque momento del trattamento, opera anche nel momento antecedente all’inizio del trattamento stesso, seppure *sub specie* di prin-

³² Si vedano, tra gli altri, F. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in ID (a cura di), *Intelligenza artificiale*, cit., 119; S. CALZOLAIO, voce “Protezione dei dati personali”, in *Dig. Disc. Pubbl.*, Torino 2017, 53; G. D’ORAZIO, *Protezione dei dati by default e by design*, in S. SICA - V. D’ANTONIO - G. M. RICCIO, *La nuova disciplina europea della privacy*, Milano 2016, 79 ss.

³³ In quest’ottica l’art. 3 del Codice era metro di selezione *ex ante* dei dati da trattare “riducendone al minimo l’utilizzazione”. Specificamente, parte della dottrina aveva interpretato la disposizione restrittivamente, come mero criterio di organizzazione tecnica degli archivi informatici. Si veda S. NIGER, *Il diritto alla protezione dei dati personali*, in J. MONDUCCI - G. SARTOR, (a cura di), *Il codice in materia di protezione dei dati personali: commentario sistematico al D. Lgs. 30 giugno 2003 n. 196*, Padova 2004, 12-13. In egual modo, R. ACCIAI - S. MELCHIONNA, *Le regole generali per il trattamento dei dati personali*, in R. ACCIAI (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla pri-*

vacy alla luce del nuovo codice, Milano 2004, 71, evidenziano come « se, da un lato, l’art. 11 pone delle regole valide per tutti i trattamenti, dall’altro, l’art. 3 ne specifica il contenuto per quelli effettuati mediante l’impiego di sistemi informativi e programmi informatici ».

Altra parte della dottrina, invece, aveva sussunto nella fattispecie — interpretando il testo estensivamente — anche i trattamenti effettuati tramite sistemi non automatizzati. Così, secondo F. D. BUSNELLI, *Commento all’art. 3*, in M. BIANCA - F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 (« Codice della privacy »)*, Padova 2017, spec. 33, « l’art. 3 parla di “sistemi informativi” in senso generale, anziché di sistemi informatici. Il suo terreno elettivo di applicazione è quello dei contesti informatici e telematici, nei quali opera con evidenza, ma la norma non schiude la porta alla sua applicazione fuori nel mondo dell’elettronica. Deve anzi ritenersi che, per un titolare di trattamento, risponde ai criteri di diligenza e di correttezza nel trattamento dare spontanea attuazione al principio di

cipio di *privacy by default* (o di necessità, che di quest'ultimo è antecedente ³⁴).

Di qui, una prima conseguenza e conclusione: mentre il *discrimen* tra le norme succitate sembra essere il diverso ambito temporale di operatività ³⁵, il dato comune resta la specificazione, in ciascuna di esse, di un principio più generale che permea di sé l'intero sistema, in ragione del quale la limitazione del diritto alla protezione dei dati personali, per non incorrere nella declaratoria di illiceità, deve rispondere al canone di proporzionalità (*sub specie* di necessità) ³⁶.

5. UNA (DIFFICILE) SCELTA: COME SELEZIONARE I SOLI DATI NECESSARI RISPETTO AD UNA DATA FINALITÀ?

Nel caso in commento, l'Autorità ha correttamente ritenuto che le modalità con cui il trattamento era posto in essere « e, segnatamente, la raccolta di informazioni particolareggiate sull'attività dei singoli veicoli monitorati dal sistema e, indirettamente, sull'attività degli autisti cui i veicoli sono (*recte*: erano) affidati » risultano sproporzionate rispetto alle finalità, che ben avrebbero potuto « essere utilmente e legittimamente perseguit(e) con la raccolta di informazioni assai più limitate » ³⁷.

Le conclusioni del Garante — e, prima ancora, la parte motiva del provvedimento — portano l'interprete ad interrogarsi in merito al procedimento logico che dovrà orientare anzitutto il titolare del trattamento ed, eventualmente, il soggetto tributario del potere di sindacare la scelta da questi presa, per non incorrere in una declaratoria di illiceità per la sproporzione tra i dati trattati e i fini perseguiti (*id est* per violazione del principio di minimizzazione).

Ebbene, il principio di cui all'art. 5, par. 1, lett. c) del Regolamento, nel prevedere che i dati devono essere pertinenti, adeguati e limitati a

necessità anche in caso di trattamento non automatizzato di dati ». In egual modo, G. RESTA, *Il diritto alla protezione dei dati personali*, in F. CARDARELLI - S. SICA - V. ZENO ZENCOVICH (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano 2004, spec. 46, rileva come « lo stesso lessico legislativo induce a valorizzare maggiormente la portata di questa norma, che attiene certamente ad un rilevante problema di tecnologie [...] ma assume anche una valenza più ampia ».

³⁴ L'art. 3 del d. lgs. 196/2003, che conteneva la definizione delle PET (*privacy enabling technologies*), ha certamente anticipato i concetti di *privacy by default* e *privacy by design*. Per un approfondimento M. MAGLIO - M. POLINI - N. TILLI (a cura di), *Manuale di diritto alla protezione dei dati personali*, Santarcangelo di Romagna (RN) 2017, 149-150.

³⁵ In egual modo in passato, quanto ai rapporti tra l'art. 11 e 3 del Codice, per assicurare autonomia alle disposizioni *de quibus*, taluni ne avevano colto il *discrimen*

nel momento temporale: mentre il principio di necessità governava la selezione dei dati « in un momento antecedente all'avvio dell'attività di trattamento » i requisiti di cui all'art. 11 del d.lgs. n. 196 del 2003 avrebbero dovuto essere accertati « nel corso del trattamento, a partire dalla raccolta ». Seguendo tale criterio di distinzione, si era sostenuto che sarebbe stato quindi prospettabile « che ad una constatazione che faccia ritenere rispettato il principio di necessità faccia seguito una valutazione negativa che porti a constatare come non pertinente o non indispensabile un determinato dato, a seconda del singolo adempimento o del soggetto interessato »; così, G. BUTTARELLI, *Commento all'art. 3 d.lgs. 196/2003*, in C. M. BIANCA - F.D. BUSNELLI (a cura di), *La protezione dei dati personali*, cit., 33.

³⁶ Per un approfondimento, si veda, G. RESTA, *Il diritto alla protezione dei dati personali*, in F. CARDARELLI - S. SICA - V. ZENO ZENCOVICH, (a cura di), *Il codice*, cit., 48.

³⁷ V. punto 3 del provvedimento.

quanto necessario per il raggiungimento della finalità, sottende una valutazione quantitativa e qualitativa dei dati rispetto allo scopo che il titolare persegue nel porre in essere un determinato trattamento ³⁸.

Nel dettaglio, la struttura della disposizione assume particolare rilievo per la commistione tra analisi di natura tecnico-scientifica e valutazioni “intessute di giudizi di valore” ³⁹.

In particolare, la valutazione della pertinenza si sostanzia in un giudizio di fatto sulla « idoneità strumentale del mezzo » ⁴⁰; prosaicamente: coerenza dell’ambito concettuale del mezzo (i dati) rispetto a quello del fine (ossia del risultato pratico perseguito).

Non si supera tale varco di controllo allorché si concluda che il mezzo sia assolutamente inutile e inappropriato o dannoso per la realizzazione del fine; se il mezzo, invece, realizza anche solo parzialmente lo scopo, allora occorrerà procedere oltre, con il giudizio sull’adeguatezza.

Così ricostruito il primo *step* di giudizio, correttamente l’Autorità ha ritenuto che i dati oggetto di trattamento superano il primo vaglio di controllo.

Sussiste, in altri termini, un nesso di ragionevole strumentalità del mezzo rispetto alle finalità summenzionate: i dati (la posizione dei veicoli acquisita dal sistema ogni 120 secondi, il loro stato fermo o in movimento, la velocità, le ore di impegno e di guida, le ore di pausa, la velocità media) sono pertinenti rispetto agli scopi del trattamento.

Riconosciuta la pertinenza dei dati, non paiono porsi problemi circa lo scrutinio di adeguatezza, sussistente, sia pure non effettuato esplicitamente dal Garante *privacy* ⁴¹, quanto piuttosto rispetto al terzo *step* di giudizio: il controllo di necessità del trattamento.

In particolare, secondo il modello trifasico di derivazione tedesca, il controllo di necessità rappresenta il secondo momento dello scrutinio di

³⁸ Sul principio di proporzionalità come criterio non solo quantitativo ma anche qualitativo si vedano, tra gli altri, S. DE NITTO, *A proposito della proporzionalità come criterio giuridico*, in *Riv. Trim. dir. pubbl.*, 2017, 1035 e A. ATTANASIO, *Principio di proporzionalità dell’azione amministrativa e libertà fondamentali*, in *Il merito*, il Sole 24 ore, X, 2004, 106.

³⁹ Invero, i criteri di pertinenza, adeguatezza e limitazione a quanto necessario — stante l’indeterminatezza del significato e il rinvio a elementi esterni, ricavati da dati extra-normativi — sono parametri valutativi. Per un approfondimento, tra gli altri, si vedano F. MODUGNO, *Principi generali dell’ordinamento*, in *Enc. Giur.*, XXIV, Roma 1991, 1 ss.; F. SORRENTINO, *I principi generali dell’ordinamento giuridico nell’interpretazione e nell’applicazione del diritto*, in *Dir. soc.*, 1987, 181 ss.; R. GUASTINI, *Sui principi di diritto*, in *Dir. soc.*, 1986, 601 ss.

⁴⁰ Così, G. SCACCIA, *Gli “strumenti” della ragionevolezza nel giudizio costituzionale*, Milano 2000, spec. 222. Si veda anche

G. PINO, *Proporzionalità, diritti e democrazia*, in *Dir. soc.*, 2014, 606 ss.

⁴¹ La verifica di adeguatezza merita di essere ricostruita in ottica sistematica, perché richiesta sia dall’articolo 5, par. 1, lett. c), che dall’articolo 25 del Regolamento, entrambi funzionali alla implementazione del principio di minimizzazione nel sistema. In particolare, il principio generale di cui all’art. 5, par. 1, lett. c) del Regolamento involge il rapporto tra i dati (il mezzo) e un determinato fine; esso, nel disposto di cui all’art. 25, si arricchisce di un ulteriore presidio: la raccolta dei dati necessari per ogni specifica finalità deve essere garantita, per impostazione predefinita, attraverso l’attuazione di misure tecniche e organizzative adeguate. Di qui, alcune peculiarità. La prima riguarda l’individuazione dell’oggetto del giudizio: nell’esplicazione generale del principio, la valutazione al lume del parametro d’adeguatezza involge i dati (sono i dati, invero, a dovere essere adeguati rispetto alla finalità); nella formulazione dell’art. 25, la valutazione *de qua* si focalizza sulle misure tecniche e organizzative, volte a

proporzionalità⁴², consistente nel riscontro dell'indispensabilità ed infungibilità del mezzo adoperato in relazione agli obiettivi perseguiti⁴³.

Nella sua forma embrionale l'istanza di misurabilità coincideva con il corollario della verifica di non eccessività degli strumenti impiegati, attributo della proporzionalità nel suo significato minimo, quale divieto di eccessi di misura. L'individuazione del *quantum* di dati "necessari" ovvero "non eccedenti", che differenzia, come si è avuto modo di enunciare, le disposizioni di cui agli artt. 11 del d. lgs. n.196 del 2003 e 5 del Regolamento, si coglie alla luce della stessa evoluzione del principio di proporzionalità.

Ebbene, il controllo di necessità è momento focale per vagliare l'effettiva minimizzazione dei dati; esso indaga, in negativo, che il mezzo sia il meno dannoso possibile per la realizzazione di un determinato fine.

In particolare, per l'individuazione del mezzo più mite (*id est*: il minimo mezzo) per il raggiungimento di una data finalità si può ricorrere ai modelli matematici. Infatti, ponendo « sull'asse delle ordinate la misura di realizzazione del fine e su quella delle ascisse la misura di intervento del mezzo »⁴⁴, si costruisce una funzione di *costante di utilità*. Quest'ultima

garantire che siano trattati i soli dati necessari per il raggiungimento di una data finalità. La seconda particolarità riguarda la complessificazione del giudizio di cui all'art. 25 par. 2 del Regolamento (*id est* il principio di *privacy by default*), che si struttura dinamicamente su due momenti: si muove dallo scrutinio della necessità dei dati rispetto allo scopo, per rintracciare, alla luce dell'adeguatezza, le misure tecniche e organizzative capaci di assicurare — in via predefinita — il raggiungimento del fine di minimizzazione.

⁴² Il sindacato di proporzionalità si compone di tre gradi di scrutinio: la verifica di idoneità; il controllo di necessità; la ponderazione vera e propria (cfr. G. SCACCIA, *Gli "strumenti" della ragionevolezza*, cit., 271). Non manca, però, chi lo ricostruisce diversamente. Il giudizio viene scomposto in quattro momenti da D. SCHEFOLD, *Aspetti di ragionevolezza nella giurisprudenza costituzionale tedesca*, in *Il principio di ragionevolezza nella giurisprudenza della Corte Costituzionale. Riferimenti comparatistici*, Milano 1994, 128-129; M. CARTABIA, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, relazione presentata alla Conferenza trimestrale delle Corti costituzionali italiana, portoghese e spagnola, Roma, 24-26 ottobre 2013, in www.cortecostituzionale.it, 4 ss.; in cinque *steps* da M. HEINTZEN, *Il principio di proporzionalità*, Modena 2015, 22.

In Europa è sempre più diffusa l'idea « di una sostanziale coincidenza fra principio di proporzionalità e secondo test della necessità ». Invero, « la proporzionalità

tende ad identificarsi [...] con una sola delle sue componenti: la necessità, che finisce in definitiva con l'assorbire l'idoneità. Ciò appare più evidente allorché, come impropriamente accade, la nozione di proporzionalità viene identificata con quella di mitezza »; così S. COGNETTI, *Principio di proporzionalità. Profili di teoria generale e di analisi sistematica*, Torino 2010, 228. L'Autore evoca, in particolare, la teoria del "diritto mite" (cfr. G. ZAGREBELSKY, *Il diritto mite. Legge, diritti, giustizia*, Torino 1992).

⁴³ La proporzionalità cui ci si riferisce, « che delimita dall'interno il contenuto lecito della libertà di trattamento dei dati, non va confusa con l'eventuale proporzionalità tra i mezzi adoperati nell'esercizio di detta libertà e l'interesse della controparte eventualmente leso, che è, viceversa, questione da ascrivere al bilanciamento in concreto degli interessi » (E. NAVARRETTA, *Commento sub art. 11*, in C. M. BIANCA - F. D. BUSNELLI (a cura di), *La protezione dei dati personali*, cit., 267). La delimitazione dell'ambito di applicazione della proporzionalità rispetto a quello del bilanciamento è problematica, perché la terza fase del giudizio di proporzionalità coincide con una ponderazione di interessi. Per un approfondimento e una ricostruzione storica del controllo di proporzionalità si vedano A. SANDULLI, voce "*Proporzionalità*", in S. CASSESE (a cura di), *Diz. Dir. pubbl.*, 2006, vol. V, 4643 ss.; S. VILLAMENA, *Contributo in tema di proporzionalità amministrativa*, Milano 2008, 34 ss.

⁴⁴ Riflessioni di Z. YI, *Das Gebot der Verhältnismäßigkeit*, Frankfurt a. M. 1998, 132.

altro non sarebbe che la « retta che unisce tutti i punti nei quali un aumento nella predisposizione dei mezzi produce una più ampia realizzazione del fine [...]. Su analoghe basi, ponendo sull'asse delle ordinate la misura di impedimento all'attuazione del fine e su quella delle ascisse la misura di impiego del mezzo » si potrebbe arrivare « ad esprimere la costante di disutilità, rappresentabile graficamente con una retta che unisce tutti i punti nei quali un più intenso utilizzo del mezzo produce una compromissione del fine. In tal senso il principio di necessità si risolve in un imperativo di minimizzazione del mezzo »⁴⁵.

Se il mezzo non è inutile e non produce un risultato disfunzionale — perché qualora così fosse esso non sarebbe, di tutta evidenza, neppure necessario — occorre individuare tutti i mezzi che, in via alternativa, permettano di realizzare uno stesso fine.

Evidentemente ciò è possibile se e nella misura in cui il mezzo originariamente individuato sia fungibile con un altro mezzo che porti alla realizzazione dei medesimi effetti, ma, al contempo, determini ricadute minori sui diritti e le libertà degli interessati.

Conseguentemente, in via di prima approssimazione, un mezzo deve ritenersi necessario se non è possibile scegliere — perché esso non esiste, o perché esiste ma non è meno incisivo sui diritti e le libertà degli interessati — un mezzo alternativo⁴⁶.

Ebbene, nell'operare il giudizio di proporzionalità (*sub specie* di necessità) il Garante — non del tutto correttamente, a nostro avviso — pare sovrapporre la valutazione delle modalità con cui il trattamento viene posto in essere con lo scrutinio relativo ai dati oggetto di trattamento.

Le disposizioni che l'Autorità ritiene essere state violate dalla società (in particolare, artt. 11, comma 1 lett. d) del Codice e 5, par. 1, lett. c) del Regolamento), per vero, sanciscono l'illiceità del trattamento allorché sussista una sproporzione tra i dati — e non invece le modalità del trattamento — e le finalità per le quali sono trattati.

Le modalità dei trattamenti, che pur naturalmente devono essere prese in considerazione, involgono un ulteriore giudizio volto ad indagare se la raccolta, la registrazione, la strutturazione, la conservazione e ogni altra operazione di trattamento siano proporzionate rispetto alla medesima finalità.

Potrebbe al più sostenersi che, anche alla luce della rubrica della norma di cui all'art. 11 d. lgs. n.196 del 2003, oggi abrogato, « modalità del trattamento e requisiti dei dati », l'interprete possa operare una commistione tra i due giudizi. È però evidente che, mentre i disposti di cui al comma 1, lettere a), b) ed e) fanno espressa menzione alle operazioni del trattamento⁴⁷ e quindi alle modalità tramite le quali i dati vengono

⁴⁵ *Ibidem*.

⁴⁶ Numerosi in dottrina sono i tentativi di individuazione, con parametri oggettivi, della necessità del mezzo. Tra gli altri, S. DE NITTO, *A proposito della proporzionalità*, cit., 1035. Si veda altresì G. SCACCIA, *Gli "strumenti" della ragionevolezza*, cit., 279 ss.; in particolare, l'Autore sottolinea che « più persuasiva delle soluzioni [...]

prospettate è la proposta [...] di scegliere il mezzo più mite secondo un ordine di preferenze che varia a seconda della combinazione qualitativa dei mezzi e della loro omogenea o disomogenea idoneità a realizzare un fine » (spec. 282).

⁴⁷ In particolare, ai sensi del comma 1, dell'art. 11 d.lgs. n.196 del 2003: « I dati personali oggetto di trattamento sono: a)

trattati, quelli di cui al comma 1 lettere c) e d) ineriscono, invece, esclusivamente ai requisiti dei dati ⁴⁸.

Del resto, lo stesso Garante nel dispositivo del provvedimento riscontra la violazione non solo della lett. d), comma 1, dell'art. 11 del Codice, ma anche del disposto di cui alla lettera a) del medesimo comma, secondo cui i dati personali devono essere « trattati in modo lecito e secondo correttezza ».

In definitiva, pertanto, condivisibile è la conclusione — così come emerge dal dispositivo — cui giunge il Garante, che ha ritenuto, da un lato, il trattamento dei dati illecito *tout court* ai sensi dell'art. 11, comma 1, lett. a) (per la sproporzione tra le modalità di trattamento e le finalità perseguite), dall'altro, illecito per la sproporzione tra i dati e le medesime finalità.

Se così è, tuttavia l'Autorità avrebbe dovuto, anche nel corpo del provvedimento: o motivare utilizzando come parametro anche l'art. 11, comma 1, lett. a) del Codice; ovvero ritenere violato il solo disposto di cui all'art. 11, comma 1, lett. d) e conseguentemente operare esclusivamente una valutazione sui requisiti dei dati e non, invece, sulle modalità di trattamento dei dati stessi.

Precisata in tali termini, deve ritenersi pur sempre corretta la conclusione, cui è addivenuta l'Autorità, del difetto di proporzione, *sub specie* di necessità: « gli scopi rappresentati dalla società [...] potrebbero essere utilmente e legittimamente perseguiti con la raccolta di informazioni assai più limitate ». Invero, dallo scrutinio di tutti i mezzi che in via alternativa permettono di realizzare lo stesso fine, può sostenersi che quello prescelto sia non necessario: esso ben può essere sostituito con altro mezzo che porti alla realizzazione degli stessi effetti ma, al contempo, determini ricadute minori sui diritti e le libertà degli interessati.

A conferma, basti pensare a come il medesimo risultato ben sarebbe raggiungibile anche senza un monitoraggio costante e anelastico, come quello effettuato dalla società, impedibile tramite l'implementazione della funzione di disattivazione della geolocalizzazione ⁴⁹.

trattati in modo lecito e secondo correttezza; raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; [...] e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati ».

⁴⁸ Tali argomentazioni possono essere riproposte a maggior ragione con riferimento all'art. 5 del Regolamento, ove neppure la rubrica dell'articolo indirizza l'interprete verso un intreccio tra il giudizio sui dati e quello sulle modalità di trattamento. Con riferimento all'art. 5 del Regolamento dovrebbe ritenersi che, mentre il par. 1 lettere a), b), e) e f) sono riferiti alle modalità di trattamento, i disposti di cui al par. 1, lettere c) e d) involgono invece i requisiti dei dati.

⁴⁹ Cfr. punto 3 del provvedimento ivi in commento, ove si legge che la sproporzione è ravvisabile anche in considerazione del fatto che « la società non ha — quantomeno — adottato il pur disponibile dispositivo di disattivazione della rilevazione geografica durante le pause consentite dell'attività lavorativa (c.d. funzione Privacy) ». Inoltre, « nel rispetto del principio di necessità (artt. 3 e 11, comma 1, lett. d), del Codice), la posizione del veicolo di regola non dovrebbe essere monitorata continuamente dal titolare del trattamento, ma solo quando ciò si renda necessario per il conseguimento delle finalità legittimamente perseguite » cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento di carattere generale in materia di localizzazione dei veicoli nell'ambito del rapporto di lavoro*, 4 ottobre 2011, n. 370, doc. web. n.1850581, in www.garanteprivacy.it.

6. CONSIDERAZIONI CONCLUSIVE.

Come si è detto nelle pagine precedenti, sulla scorta dei principi di finalità del trattamento, minimizzazione dei dati, *privacy by design*, espressamente richiamati (o da leggere in trasparenza nel testo del provvedimento), l'Autorità ha correttamente vagliato e rilevato la illiceità del trattamento, utilizzando come parametri di riferimento, in combinato disposto, le disposizioni nazionali e sovranazionali.

Ebbene, se il giudizio sulla illiceità del trattamento, condotto tramite l'applicazione dei principi cardine in materia di protezione dei dati personali, è occasione di consolidamento e conferma di schemi argomentativi già applicati dal Garante, per un verso, nuovo è il rilievo che essi assumono al lume della disciplina regolamentare; per altro verso, rilevante è l'approccio dell'Autorità che, in ottica di effettiva tutela dei diritti e delle libertà degli interessati, ne prescrive il rispetto, non solo al titolare del trattamento, ma anche al fornitore del servizio, finanche incidendo direttamente sulla sua libertà d'impresa.

In ciò può leggersi il bilanciamento che la nuova disciplina in materia di protezione dei dati sottende e richiede: quello tra libera circolazione dei dati e tutela degli interessati; il che, in sostanza, è come dire tra mercato e persona.

NOEMI MINISCALCO