Attività ispettiva del Garante Privacy e collaborazione della Guardia di Finanza

GIOVANNI RECCIA

Colonnello della Guardia di Finanza, plurilaureato ed abilitato alle professioni di avvocato, di revisore legale dei conti e di giornalista pubblicista, già comandante del Nucleo Frodi Tecnologiche

FABIO PASCUCCI

Dottore in Giurisprudenza, Scienze politiche, Economia e Scienze della sicurezza economico finanziaria, è Ufficiale superiore della Guardia di Finanza e ha svolto numerosi incarichi pluriennali presso Uffici e C.E.D. del settore informatico

1. I poteri di indagine del Garante

Dal 1997, con l'entrata in vigore della Legge 675/1996, in seguito sostituita dal Decreto legislativo 30 giugno 2003, n.196, opera il Garante per la protezione dei dati personali, quale Autorità amministrativa indipendente istituita per assicurare la tutela dei diritti e delle libertà fondamentali nel trattamento dei dati personali, nel rispetto della dignità degli individui; la stessa rappresenta anche l'Autorità di controllo designata ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679.

Nel caso in cui i trattamenti violino le disposizioni del Regolamento, può rivolgere ammonimenti al titolare del trattamento o al responsabile del trattamento e ingiungere di conformare i trattamenti alle disposizioni del Regolamento, svolgendo correttamente il trattamento nel rispetto dei diritti e delle libertà fondamentali degli individui. Inoltre, può imporre una limitazione provvisoria o definitiva del trattamento, nonché ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento. Può inoltre vietare, anche d'ufficio, i trattamenti illeciti o non corretti ed eventualmente disporre il blocco. Può richiedere al titolare e al responsabile del trattamento, all'interessato e a terzi di fornire informazioni e di esibire documenti, nonché

disporre accessi alle banche dati o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorra effettuare rilevazioni comunque utili al medesimo controllo.

Il Garante, pertanto, controlla¹ se il trattamento dei dati personali da parte di enti privati o pubblici avvenga in modo lecito e corretto. I suoi poteri, ai sensi dell'art. 58 del Regolamento, si suddividono in:

- a. poteri di indagine (art. 58, co.1);
- b. poteri correttivi (art. 58, co.2);
- c. poteri autorizzativi e consultivi (art. 58, co.3).

Nell'esecuzione dei compiti di indagine, può ingiungere di fornire ogni informazione di cui abbia bisogno. Pertanto, può ottenere l'accesso a tutti i dati personali e a tutte le informazioni necessarie, nonché a tutti i locali del titolare e del responsabile del trattamento, compresi gli strumenti e i mezzi di trattamento dei dati.

Nella fase prodromica all'accertamento stesso, viene riconosciuto anche il potere di notificare le presunte violazioni del Regolamento nei confronti del titolare/responsabile del trattamento, informando il medesimo sulle indagini che l'Autorità sta compiendo.

I controlli correttivi spaziano dal semplice avvertimento (tradotto in un ammonimento al titolare/responsabile) che eventuali trattamenti possano verosimilmente violare il regolamento, ad atti che incidono direttamente sull'operatività connessa al trattamento dei dati. Come accennato, in tale ambito, può essere imposta una limitazione, provvisoria o definitiva, al trattamento, fino ad includere anche il divieto stesso di trattamento. Si possono anche revocare le certificazioni o ingiungere all'organismo di certificazione di ritirare le certificazioni rilasciate, se i requisiti non sono soddisfatti, nonché ordinare la rettifica, la cancellazione o l'aggiornamento dei dati personali.

Disponendo la rettifica, la cancellazione di dati personali o la limitazione del trattamento, si pongono divieti alle attività inerenti ai trattamenti fino alla revoca della certificazione (o ingiungere all'organismo di certificazione di ritirarla o di non rilasciarla) nel caso in cui si giunga alla conclusione che, dati gli eventi, i requisiti a suo tempo riconosciuti non sono o non sono più soddisfatti. Si potrà ingiungere al titolare o al responsabile del trattamento di

¹ E. BARRACO e A. STIZIA, *Potere di controllo e privacy*, Ipsoa, Milano 2016; M. MANDICO, *Privacy e GDPR: manuale applicativo con esempi e casistiche settoriali*, Maggioli Editore, Rimini, 2019; N. BERNARDI, *Privacy. Protezione e trattamento dei dati*, Ipsoa, Milano 2019; M. GIORDANO e R. LANZO, *Data breach e privacy*, Key editore, Milano, 2020.

soddisfare le richieste dell'interessato di esercitare i relativi diritti o ordinare al medesimo soggetto di conformare i trattamenti alle norme, specificando eventualmente le modalità e i termini per la conformità. È prevista perfino la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

I poteri autorizzativi e consultivi, a loro volta, vanno dalla consulenza al titolare del trattamento, a funzioni tipiche dell'Autorità cui è demandato il compito di rilasciare autorizzazioni: il rilascio di pareri su progetti di codici di condotta e l'approvazione degli stessi, la convalida dei criteri di certificazione e ancora l'adozione delle clausole-tipo di protezione. Tutte attività che hanno la precipua funzione di costruire l'assetto organizzativo entro il quale dovrà poi esercitarsi l'attività del titolare/responsabile finalizzata al corretto trattamento dei dati.

L'Ufficio del Garante può svolgere attività istruttorie in relazione a segnalazioni o reclami proposti. Detto Ufficio, infatti, riceve ed esamina i reclami e le segnalazioni, provvedendo sui ricorsi presentati dagli interessati. Nell'esaminare i reclami, le segnalazioni e i ricorsi, esegue anche accertamenti e verifiche su richiesta del cittadino. Quest'ultimo, tuttavia, può sempre tutelare i propri dati personali, in primo luogo, esercitando i diritti previsti dagli articoli da 15 a 22 del Regolamento (UE) 2016/679. L'interessato può presentare un'istanza al titolare, ad esempio, mediante lettera raccomandata, PEC, posta elettronica, ecc., che può essere riferita, a seconda delle esigenze del medesimo, a specifici dati personali, a categorie di dati o ad un particolare trattamento, oppure a tutti i dati personali che lo riguardano, comunque trattati. Se il soggetto ritiene che il trattamento dei dati che lo riguardano non sia conforme alle disposizioni vigenti ovvero se la risposta ad un'istanza con cui esercita uno o più dei diritti previsti dagli articoli 15-22 del Regolamento (UE) 2016/679 non sia pervenuta nei tempi previsti (senza ingiustificato ritardo, al più tardi entro un mese dal suo ricevimento. Tale termine può essere prorogato di due mesi, in virtù della complessità e del numero di richieste) o non è soddisfacente, l'interessato può rivolgersi all'Autorità giudiziaria o al Garante per la protezione dei dati personali, in quest'ultimo caso mediante un reclamo ai sensi dell'articolo art. 77 del Regolamento (UE) 2016/679.

Quindi chiunque può rivolgere, ai sensi dell'art. 144 del Codice in materia di protezione dei dati personali, una segnalazione che il Garante può valutare anche ai fini dell'emanazione dei provvedimenti di cui all'art. 58 del Regolamento, cui si aggiunge il reclamo che, invece, è lo strumento che consente all'interessato di rivolgersi al Garante per lamentare una violazione della disciplina in materia di protezione dei dati personali (art. 77 del

Regolamento (Ue) 2016/679 e artt. da 140-bis a 143 del Codice in materia di protezione dei dati personali) e di richiedere una verifica dell'Autorità. Al reclamo segue un'istruttoria preliminare e un eventuale successivo procedimento amministrativo formale che può portare sempre all'adozione dei provvedimenti di cui all'articolo 58 del Regolamento.

2. Le ispezioni d'iniziativa in ragione del rischio privacy

Sul finire del 2020² è stata predisposta l'attività ispettiva a cura dall'Ufficio del Garante della Privacy, anche per mezzo della Guardia di finanza, relativamente al periodo gennaio-giugno 2021. La predetta attività prende le mosse dalla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione dei dati. In particolare, è emersa l'esigenza di individuare specifici temi di indagine nell'ambito dei nuovi scenari della società moderna anche alla luce degli effetti derivanti dall'emergenza sanitaria nazionale legata alla diffusione di Sars-Cov-2 e della conseguente crisi sanitaria che ne è seguita. Di conseguenza, si è rilevata un'amplificazione dei rischi connessi alla maggiore dipendenza da dati e tecnologie anche in termini di concentrazione del potere di mercato e di sorveglianza, rendendo evidente la necessità di efficaci meccanismi di garanzia a salvaguardia dei diritti e delle libertà fondamentali all'esito di opportune iniziative conoscitive, anche di tipo ispettivo.

Per il periodo gennaio-giugno 2021, il compito ispettivo è stato indirizzato verso:

- a. accertamenti in riferimento a profili di interesse generale nell'ambito di:
 - trattamenti di dati biometrici per il riconoscimento facciale anche mediante sistemi di videosorveglianza. Il dato biometrico è un dato personale relativo alle caratteristiche fisiche, fisiologiche o comportamentali di un individuo mediante il quale ne consente l'identificazione univoca³. Nello specifico, il dato biometrico può essere utilizzato per attività di profilazione (per esempio le abitudini dei clienti), per la sorveglianza in determinati luoghi (si pensi alla scansione della retina per accedere in un locale strettamente riservato), o semplicemente per attività quotidiane (la scansione dell'impronta digitale per lo sblocco del proprio smartphone). Il dato biometrico, se correttamente trattato, può essere molto utile per garantire maggiore sicurezza e tutela nella prevenzione di frodi e accessi abusivi, tuttavia un errato trattamento

² Deliberazione del 10 dicembre 2020 dell'Autorità Garante per la protezione dei dati personali.

³ G. ZICCARDI e P. PERRI, *Dizionario Legal Tech*, Giuffrè, Milano 2020.

dei dati può dar luogo a compromissioni della reputazione, dell'integrità fisica o degli interessi economici⁴;

- trattamenti di dati personali nel settore della c.d. “videosorveglianza domestica” e nel settore dei sistemi audio/video applicati ai giochi (c.d. giocattoli connessi). L'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento, quali le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata o in materia di controllo a distanza dei lavoratori. L'attività di videosorveglianza va effettuata tenendo conto del cosiddetto principio di minimizzazione dei dati riguardo alla scelta delle modalità di ripresa e dislocazione delle telecamere sulla base delle specifiche finalità perseguite e deve raccogliere e trattare solo i dati personali pertinenti e non eccedenti le finalità stesse. Per quanto concerne il settore dei sistemi audio/video applicati ai giochi, si potrebbe fare riferimento a *smart toys* che uniscono ad un elemento fisico, come un apparato elettronico per bambini, un elemento tecnologico in grado di connettersi ad internet e di scambiare i dati di gioco con un server esterno che offre, ad esempio, la possibilità di ricevere nuovi contenuti in tempo reale;
- trattamenti di dati personali effettuati da “data broker”. Si tratta di dati personali elaborati dai c.d. information brokers, data providers e data suppliers, ovvero aziende che raccolgono i dati direttamente o li acquistano da altre aziende (es. banche, circuiti di carte di credito, finanziarie, etc.), e aggregano tali informazioni con dati provenienti da altre fonti (ad esempio società di informazioni creditizie). Pertanto, recuperano informazioni on line da fonti pubbliche, le aggregano, le interpretano e le analizzano per poi venderle sul mercato. Nel caso in cui i dati vengono venduti a imprese che intendono realizzare campagne pubblicitarie mirate e/o offrire servizi personalizzati, l'attività del data broker può essere molto invasiva e comportare enormi rischi privacy;
- trattamenti di dati personali effettuati da società rientranti nel settore denominato “Food Delivery”. Proprio la pandemia ha impresso un deciso cambiamento nelle nostre abitudini, a causa della limitazione negli spostamenti, il mantenimento della distanza sociale, il lockdown, con inevitabili effetti sul restringimento alla normale frequentazione di bar, ristoranti, pub, favorendo, al contrario, il proliferare di piatta-

⁴ S. GIRARDI, *Dati biometrici. Quo vadis per un trattamento legittimo?*, ALTALEX, Milano 2021.

- forme online per la vendita di alimenti da consegnare a domicilio;
- *data breach*. Un *data breach* non solo è un evento doloso come un attacco informatico, ma può essere anche un evento accidentale come un accesso abusivo ovvero un incidente (es. un incendio o una calamità naturale, la perdita di una chiavetta USB o la sottrazione di documenti con dati personali. L'art. 4 del regolamento europeo definisce la violazione dei dati personali (*data breach*) come “*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*”. In base all'art. 33 del GDPR, in caso di violazione dei dati il responsabile del trattamento, se designato, deve avvertire il titolare dell'avvenuta violazione dei dati. Quest'ultimo dovrà, a quel punto, notificare l'evento all'autorità di controllo. tranne che nel caso in cui “*sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*”;
 - b. controlli nei confronti di titolari del trattamento di dati personali, pubblici e privati, appartenenti a categorie omogenee in relazione alla verifica dei presupposti di liceità del trattamento e alle condizioni per il consenso qualora il trattamento sia fondato su tale base giuridica, sul rispetto dell'obbligo dell'informativa nonché sulla durata della conservazione dei dati. Ciò, prestando anche specifica attenzione a profili sostanziali del trattamento che esplicano significativi effetti sugli interessati.

3. La collaborazione con la guardia di finanza

L'attività ispettiva programmata con la recente deliberazione riguarda n. 50 accertamenti ispettivi di iniziativa effettuati anche mediante delega alla Guardia di finanza. Sulla base dell'art. 3 del Decreto legislativo 19 marzo 2001, n. 68, il 30 marzo 2021 è stato sottoscritto, rinnovando il precedente, un Protocollo d'intesa relativo ai rapporti di collaborazione tra il Garante per la protezione dei dati personali e la Guardia di finanza per cui le ispezioni in materia di trattamento dei dati personali vengono effettuate attraverso:

- il reperimento di dati e informazioni sui soggetti da controllare;
- la partecipazione di proprio personale agli accessi alle banche dati, ispezioni, verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati;
- l'assistenza nei rapporti con l'Autorità Giudiziaria;
- lo sviluppo di attività delegate o sub-delegate per l'accertamento delle violazioni in materia di protezione dei dati personali;

- la partecipazione di proprio personale, a richiesta del Garante, a ispezioni congiunte con Autorità di protezione dei dati personali appartenenti ad altri Paesi. Considerata la necessità di aumentare l'efficacia dell'attività di vigilanza e controllo sul rispetto della disciplina svolta dall'Ufficio del Garante, con particolare riferimento alla prevenzione e all'accertamento delle violazioni commesse nei nuovi contesti tecnologici, il predetto Ufficio si avvale dell'attività altamente specialistica fornita dal Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza.

Le attività svolte d'intesa tengono conto dell'evoluzione del quadro normativo, delle tecnologie informatiche e digitali e delle tecniche di informazione e di comunicazione.

La Guardia di Finanza collabora altresì:

- a. nell'esecuzione di indagini conoscitive sullo stato di attuazione della legge in determinati settori;
- b. nell'esecuzione, a richiesta del Garante, di verifiche on-line, codificate sulla base di uno o più provvedimenti del Garante, volte a rilevare, dall'esame dei siti web e degli altri strumenti telematici utilizzati, il rispetto della disciplina di protezione dei dati personali da parte dei titolari, pubblici e privati, che effettuano trattamenti di dati personali per mezzo di reti telematiche;
- c. alla progettazione e attuazione, d'intesa con il Garante, di altre iniziative, anche nell'ambito della cooperazione internazionale;
- d. nell'attività di notifica degli atti e dei provvedimenti adottati nell'esercizio dei poteri di cui all'art. 58 del Regolamento (UE) 2016/679.

La Guardia di Finanza provvede inoltre a segnalare al Garante tutte le situazioni rilevanti ai fini dell'applicazione del D.Lgs. 30 giugno 2003, n. 196, di cui venga a conoscenza nel corso dell'esecuzione delle ordinarie attività di servizio.

Quando ritenuto necessario per agevolare le attività istruttorie successive alle ispezioni, il personale del Garante, specificamente incaricato, partecipa alle attività delegate alla Guardia di Finanza. Naturalmente, detto personale addetto all'Ufficio del Garante sarà tenuto al segreto d'ufficio su tutto ciò di cui sia venuto a conoscenza, nell'esercizio delle proprie funzioni, in ordine a banche di dati e a operazioni di trattamento, rivestendo, secondo determinate modalità, la qualifica di ufficiale o agente di polizia giudiziaria (art 156, commi 8 e 9 del D.Lgs. 30 giugno 2003, n. 196).

Di contro, ovviamente, il personale della Guardia di Finanza, che collabora con il Garante, è tenuto al segreto su tutto ciò di cui sia venuto a conoscenza nel corso delle attività di collaborazione.

Il Garante, in relazione alle questioni su cui ritenga necessario avvalersi della collaborazione, invia specifiche richieste al Gruppo Privacy del Nucleo Speciale della Guardia di Finanza, il quale assicura, con proiezione nazionale, gli adempimenti connessi all'attività collaborativa, avvalendosi anche dei reparti del Corpo dislocati sul territorio, i quali riferiscono al Garante per tramite del Gruppo.

Sempre per il tramite del Gruppo della GdF, il Garante può richiedere la collaborazione delle altre articolazioni del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche per tutte quelle attività ispettive che richiedano un'elevata specializzazione in ambito telematico. Quest'ultimo, infatti, comprendendo al proprio interno anche l'aliquota di personale dedicata al contrasto alle frodi tecnologiche, può impiegare direttamente il citato personale per tutti quei servizi in cui servano specifiche competenze in ambito IT (*Information Technology*).

In relazione alle richieste di collaborazione, sono fornite al Gruppo Privacy documenti, informazioni ed elementi necessari per eseguire le attività ispettive delegate. Le richieste devono essere molto specifiche e indicano l'ambito e lo scopo dell'intervento, i soggetti interessati, i fatti, le circostanze e le modalità in ordine ai quali è chiesto di reperire i dati e le informazioni, di fornire assistenza, di partecipare all'esecuzione delle attività ispettive e/o di sviluppare le attività delegate o sub-delegate per l'individuazione delle violazioni di natura amministrativa o penale ed ogni altra utile informazione. Gli esiti dei controlli vengono riferiti dal Gruppo Privacy esclusivamente al Garante, unitamente alla documentazione acquisita, fermo restando gli obblighi di denuncia ai sensi dell'art. 347 del c.p.p. Allo stesso modo, le segnalazioni di tutte le situazioni rilevanti di cui vengano a conoscenza i Reparti della Guardia di Finanza sul territorio nazionale nel corso dell'esecuzione delle ordinarie attività di servizio, sono segnalate al Garante esclusivamente per il tramite del Gruppo Privacy.

Nello specifico, l'attività ispettiva si sostanzia in una serie di informazioni da acquisire in via preventiva o nell'immediatezza dell'intervento. Il soggetto interessato viene invitato a rappresentare e comunicare:

- struttura e organizzazione della società;
- distribuzione delle funzioni in materia di protezione dei dati personali;
- modalità con la quale viene fornita agli interessati l'informativa di cui agli art. 13 e 14 del Regolamento generale sulla protezione dei dati (UE) 2016/679, con relativa documentazione;

- modalità di acquisizione dei consensi ai sensi degli artt. 7 e 8 del Regolamento generale sulla protezione dei dati (UE) 2016/679, per le ulteriori finalità (marketing – profilazione – comunicazione dei dati a soggetti terzi) con relativa documentazione;
- istituzione del registro dei trattamenti, mettendone a disposizione copia dello stesso (art. 30 del Regolamento generale sulla protezione dei dati (UE) 2016/679);
- designazione di responsabili esterni e/o sub responsabili) del trattamento con acquisizione del relativo contratto e designazione (art. 28 del Regolamento generale sulla protezione dei dati (UE) 2016/679);
- nomina del Data Protection Officer (DPO) in relazione agli artt. 37 e segg. del Regolamento generale sulla protezione dei dati (UE) 2016/679;
- soggetti autorizzati ad accedere ai dati personali oggetto del trattamento e documentazione relativa all'istruzione e alla formazione degli incaricati, con copia delle relative nomine (art. 29 del Regolamento generale sulla protezione dei dati (UE) 2016/679);
- tipologia di profilazione effettuata e descrizione dettagliata del suo funzionamento, con particolare riferimento alle modalità di raccolta, di aggregazione e di analisi dei dati personali della clientela;
- utilizzo a fini di profilazione di dati particolari dell'interessato (art. 9 del Regolamento generale sulla protezione dei dati (UE) 2016/679);
- tipologia di attività di marketing effettuato a seguito della profilazione;
- il periodo di conservazione dei dati di profilazione personali ovvero i criteri utilizzati per determinare tale periodo;
- valutazione d'impatto eventualmente effettuata in relazione ai trattamenti dei dati oggetto della profilazione;
- presupposti, ambito e modalità di comunicazione a terzi dei dati, anche in riferimento ad eventuali società controllanti, controllate o collegate ed all'eventuale trasferimento dei dati in paesi non appartenenti all'Unione Europea;
- procedure poste in essere per l'esercizio dei diritti degli interessati (artt. 15-22 del Regolamento generale sulla protezione dei dati (UE) 2016/679);
- misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento generale sulla protezione dei dati (UE) 2016/679) con particolare riferimento a:
 - pseudoanonimizzazione e cifratura dei dati personali;
 - capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi del trattamento;
 - capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento;
- principali applicazioni utilizzate sui sistemi (client server/web application);
- misure idonee per accedere a banche dati (username e password; strong authentication);
- audit effettuato sia internamente che presso responsabili esterni;
- alert implementati su sistemi;
- backup sui dati.

È da aggiungere che l'art. 3 del D.Lgs. n. 68/2001 consente alla Guardia di Finanza di procedere, nel corso di ispezioni amministrative, anche all'utilizzo dei poteri di polizia economica e finanziaria previsti dalle leggi e dai regolamenti vigenti a tutela degli interessi statuali ed europei. Quindi in relazione alle notizie acquisite che lasciano supporre la commissione di determinati illeciti, per acclarare la realtà dei fatti ed a seconda dei casi individuati, la Guardia di Finanza può procedere alla verifica dei libri e registri detenuti a fini contabili, nonché all'accertamento del patrimonio e delle finanze del soggetto ispezionato.

4. Conclusioni

Le sanzioni comminate dal Garante della privacy nel 2020 hanno raggiunto un valore complessivo di quasi 60 milioni di euro⁵. L'Italia è al primo posto per le sanzioni alle aziende per violazioni privacy, in Europa. Ben distanziata al secondo posto la Svezia, con 7 milioni di euro. Una recente indagine di Finbold⁶ – rivista finanziaria online – potrebbe apparentemente far giungere alla conclusione che le ingenti sanzioni applicate sono prova del funzionamento del GDPR: “le aziende sono state colpite, quindi lo strumento è efficace”. Difatti le sanzioni italiane hanno riguardato il trattamento dati dei call center (lo spam del telemarketing; le attivazioni non richieste di servizi). La sanzione del Garante Privacy comminata ad Eni Luce e Gas, ad esempio, è stata di 11 milioni e 500 mila euro ed a Tim di 27 milioni e 800 mila euro. Inoltre, ha ordinato a Roma Capitale il pagamento di una sanzione di 500mila euro per illecito trattamento di dati personali di utenti

⁵ ANSA.it, Tecnologia. Garante Privacy, quasi 60 milioni di sanzioni nel 2020, del 10 dicembre 2020.

⁶ Finance in Bold, GDPR Fines Report 2020, al sito <https://finbold.com/gdpr-fines-2020>.

e dipendenti, effettuato attraverso il sistema di prenotazione degli appuntamenti “TuPassi”⁷. Tuttavia, il dato potrebbe evidenziare anche profili diversi legati sia ad una bassa conoscenza da parte delle aziende italiane del tema privacy e della gestione dei dati, sia alla programmazione delle ispezioni, tenuto conto che circa l’85% delle sanzioni sono state applicate nei confronti di tre soli soggetti giuridici.

Il Garante, come abbiamo visto, ha deliberato il piano dell’attività ispettiva da svolgere nel primo semestre 2021, e, dopo aver individuato i settori a rischio privacy, sarebbe interessante conoscere anche i criteri utilizzati per scegliere i singoli soggetti da sottoporre ad ispezione. Nulla dice in dettaglio la stessa deliberazione periodicamente emanata dal Garante. È evidente la necessità che le ispezioni siano intraprese in maniera mirata nei confronti di soggetti preventivamente selezionati in base a precise oggettive risultanze, acquisite in esito ad analisi di contesto specifiche, espressive di un livello di rischio elevato in materia di privacy. L’attività di selezione, pur essendo espressione di una discrezionalità tecnica, potrebbe fondarsi su esigenze che si pongano in equilibrio tra la tutela dell’interesse alla privacy e la tutela della libertà del cittadino sottoposto a controllo, nella ricerca della reciproca collaborazione, tenuto conto altresì dei principi di affidamento e buona fede. Sappiamo, infatti, che la programmazione delle attività di controllo devono seguire una procedura interna che renda efficace la scelta sulla base di elementi configurabili in capo alla singola persona fisica o giuridica. Potremmo infatti individuarne i limiti, ad esempio:

- nei soggetti di rilevanti dimensioni aziendali rispetto a soggetti con volumi d’affari medi o bassi. In tale ambito il numero dei dipendenti dovrebbe influenzare la scelta più dell’aspetto economico (per quanto i due elementi tendano a coincidere);
- nella presenza numerica di aziende sul territorio nazionale, con un’equa ripartizione dei controlli tra nord, centro e sud Italia, evitando concentrazioni o, di contro, assenza di controlli in aree specifiche;
- nel tenere presente le segnalazioni pervenute all’Ufficio, distinguendo le denunce firmate da quelle anonime: queste ultime non possono costituire presupposto per la scelta del soggetto da controllare. Infatti, le segnalazioni in forma anonima costituiscono una pratica deplorabile a cui ricorre chi fugge dalle proprie responsabilità. Dal punto di vista giuridico tali denunce non possono confluire in procedimenti amministrativi;
- nel coordinamento transnazionale sui soggetti giuridici a carattere multinazionale, atteso che il trattamento dei dati eseguito in un altro

⁷ Newsletter dell’Autorità Garante per la protezione dei dati personali del 25 gennaio 2021.

Paese (vieppiù se si tratta di un Paese europeo che ha adottato il GDPR) presumibilmente vengono effettuate allo stesso modo in Italia da imprese partecipate, controllate, collegate, stabilizzate o consolidate e viceversa;

- nella ricognizione delle c.d. “fonti aperte”, siti internet e social network, per analizzare la posizione del soggetto da controllare in termini reali ed immediati (se possibile), profilo che potrebbe far emergere, ad esempio, corretti comportamenti nel trattamento dei dati non emersi *prima facie* o non presenti agli atti d’archivio;
- nel coinvolgimento in precedenti attività di Polizia Giudiziaria del selezionato, aspetto che può aggravare la posizione del soggetto preindividuato, evidenziandone una pericolosità *lato sensu*.

In sostanza, l’attività ispettiva dovrebbe conoscere un momento preliminare di programmazione volto alla calibrazione degli elementi suscettibili di rischio privacy in capo ai singoli soggetti da controllare, seppur già inclusi nei settori economici considerati a maggior rischio privacy. Va aggiunto che se la Deliberazione del Garante, che individua i settori a rischio e le conseguenti attività ispettive da svolgere, è emanata a fini di trasparenza, allo stesso modo l’esito dell’azione svolta, con i risultati conseguiti, potrebbe essere oggetto di analisi “a posteriori” nel suo complesso, da rendersi pubblica, in modo da favorire, da un lato, una maggiore consapevolezza da parte dei cittadini al diritto alla riservatezza e sicurezza dei dati e, contemporaneamente, diffondendo una maggiore cultura della privacy, dall’altro, dare efficacia reale agli indirizzi programmatici ispettivi annuali di rischio, non soltanto in termini di sanzioni comminate, bensì avendo a riferimento la complessiva azione di controllo in ambito nazionale.