Provvedimento del 17 aprile 2026 [10241537]

VEDI ANCHE Comunicato stampa del 20 aprile 2026

[doc. web n. 10241537]

Provvedimento del 17 aprile 2026

Registro dei provvedimenti
n. 237 del 17 aprile 2026

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente e il dott. Agostino Ghiglia, componenti, e il dott. Luigi Montuori, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (di seguito “Regolamento”);

VISTO il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, di seguito “Codice”);

VISTE le numerose segnalazioni e reclami pervenuti all’Autorità a partire dal mese di aprile 2024 nei confronti di Poste Italiane S.p.a. e PostePay S.p.a. concernenti l’illiceità del trattamento di dati personali degli utenti delle app Bancoposta e PostePay, installate su sistema operativo Android;

ESAMINATA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell’art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Pasquale Stanzione;

PREMESSO

1. Le segnalazioni e i reclami.

Nei mesi di aprile e maggio 2024, sono pervenute 140 segnalazioni e 12 reclami con cui è stato rappresentato a questa Autorità che gli utenti delle app Bancoposta e PostePay (installate su sistema operativo Android) sono stati destinatari di un messaggio di invito ad “autorizzare l’App ad accedere ai dati per rilevare la presenza di eventuali software dannosi”.

Il medesimo messaggio indicava che si trattava di una opzione obbligatoria, da attivare immediatamente e che, in caso di mancata attivazione, sarebbe stato possibile effettuare un numero massimo di tre accessi, oltre i quali l’operatività dell’app sarebbe stata inibita.

In particolare, nell’apposita schermata di configurazione a cui l’utente veniva indirizzato, tramite il

messaggio in questione, il rilascio dell'anzidetta autorizzazione consentiva alle applicazioni app Bancoposta e PostePay di accedere ai c.d. "dati di utilizzo", allo scopo di monitorare le applicazioni utilizzate e la loro relativa frequenza d'uso, nonché di identificare il gestore telefonico, le impostazioni relative alla lingua e "altri dati di utilizzo".

In merito alla vicenda, anche l'Autorità garante della concorrenza e del mercato (di seguito "AGCM"), in relazione ai profili di propria competenza, ha aperto un procedimento -in data 22 aprile 2024- , in materia di pratiche commerciali scorrette, ravvisando la possibile violazione degli articoli 20, 24 e 25 del Codice del consumo.

2. L'attività istruttoria.

2.1 La prima richiesta di informazioni ex art. 157 del Codice.

Con nota del 30/4/2024, Poste italiane S.p.a. e PostePay S.p.a. (di seguito anche "le Società" o "le parti") hanno fornito riscontro alla richiesta di informazioni, formulata dall'Autorità, il 16/4/2024 (prot. n. 46935), rappresentando che:

- "Poste Italiane e PostePay sono contitolari. Altresì, XX e XX operano rispettivamente quale responsabile e sub-responsabile";

- "[il trattamento] è necessario per fornire tramite le App i servizi esplicitamente richiesti dagli Interessati ed erogare tali servizi in conformità alla normativa vigente e in particolare alla disciplina applicabile in materia di servizi di pagamento, che impone d'implementare meccanismi di monitoraggio e misure tecniche volte a garantire la sicurezza delle informazioni e delle transazioni disposte tramite canali digitali. In particolare, il trattamento è implementato in adempimento delle previsioni contenute negli articoli 2 e 18 degli Standard Tecnici di Regolamentazione emanati dall'Autorità Bancaria Europea (European Banking Authority - EBA) e adottati con il Regolamento Delegato (UE) 2018/389 della Commissione Europea del 27 novembre 2017 "Norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri" ai sensi di quanto previsto dall'art. 98 della direttiva UE 2015/2366 (Direttiva PSD2)";

- "[…] i Dati raccolti sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati, poiché essi sono necessari a garantire la sicurezza delle informazioni e delle transazioni disposte dai clienti tramite le App";

- "[le informazioni di cui agli artt. 13 e 14 del RGPD] sono comunicate:

  • tramite il c.d. 'app store' in sede di scaricamento delle App;

  • in sede d'installazione e di primo accesso alle App;

  • all'interno dell'App BancoPosta nella sezione Impostazioni/Condizioni di servizio e Privacy/Informativa sul trattamento dei dati personali e nell'App PostePay nella sezione Impostazioni App/Termini e condizioni/Informativa sul trattamento dei dati personali";

- "[…] il Trattamento è svolto usando l'applicativo ThreatMetrix, fornito da XX tramite XX. ThreatMetrix è una componente della piattaforma antifrode di Poste Italiane adottante un approccio basato sul rischio che consente di analizzare in tempo reale le operazioni realizzate tramite l'App e fornire un indice di rischio associato alle operazioni stesse. In particolare, ThreatMetrix fornisce informazioni sullo stato di sicurezza dei dispositivi degli Interessati, rilevando anomalie e meccanismi di spoofing e valutando l'integrità delle applicazioni e la presenza di applicativi malevoli e tecnologie di rooting. Più nel dettaglio, solo in caso di dispositivi basati su sistema operativo Android, la libreria applicativa di

ThreatMetrix integrata nelle App, a fronte dell'autorizzazione richiesta, raccoglie un campo, per rilevare le applicazioni in esecuzione e valutare quelle malevole sul dispositivo dell'Interessato che sta effettuando operazioni di pagamento. ThreatMetrix raccoglie solo il codice hash MD5 delle applicazioni rilevate come in esecuzione. La codifica hash è un'operazione irreversibile a seguito della quale non si può risalire al dato digitale originale. La raccolta di queste informazioni è necessaria per le analisi di device reputation (livello di affidabilità del dispositivo) svolte a fini antifrode, poiché un'applicazione malevola eseguita quando l'Interessato effettua una transazione potrebbe comportare la realizzazione di atti illeciti a fini frodatori (transazioni non autorizzate, manipolazione o sostituzione d'informazioni di pagamento e sottrazione di credenziali di autenticazione). Quindi, la disponibilità di queste informazioni consente di tutelare gli Interessati, implementando misure per bloccare transazioni fraudolente effettuate tramite dispostivi compromessi";

- "[…] il Trattamento è stato attivato appunto per garantire la sicurezza delle transazioni realizzate dagli Interessati e delle informazioni a essi riferibili, in adempimento a quanto previsto dalla disciplina applicabile in materia di servizi di pagamento e dalla stessa normativa in materia di protezione dei dati personali e in particolare dall'art. 32 del RGPD. Ciò, assieme alle misure di tutela degli Interessati implementate (in particolare, la codifica delle informazioni in formato hash MD5 e l'assenza di trattamento in chiaro d'informazioni inerenti al nome delle applicazioni rilevate, a elementi multimediali o altre informazioni riservate dell'Interessato), ha condotto a escludere la presenza di un rischio elevato per i diritti e le libertà delle persone fisiche e conseguentemente la necessità di svolgere una valutazione d'impatto sulla protezione dei dati a norma dell'art. 35 del RGPD".

Con specifico riferimento all'individuazione della base giuridica che, ai sensi dell'art. 6 del Regolamento, legittimerebbe l'accesso, da parte delle app PostePay e Banco Poste, ai dati personali contenuti nei dispositivi mobili - allo scopo di rilevare, all'interno degli stessi, la presenza di eventuali malware - le Società hanno prodotto uno specifico documento nel quale sono stati richiamati, da un lato, la Direttiva UE 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno (anche nota come "Direttiva dei Sistemi di Pagamento 2" o "PSD2"), dall'altro, gli Standard Tecnici di Regolamentazione (RTS) elaborati dalla European Banking Authority, adottati con il Regolamento Delegato UE 2018/389 della Commissione europea (cfr. all. alla nota del 30/4/2024).

In tale documento, le Società hanno sostenuto che:

- "tra gli obiettivi perseguiti dalla vigente normativa in materia di servizi di pagamento vi è quello di assicurare un livello adeguato di sicurezza dei fondi e dei dati personali degli utenti mediante l'adozione di requisiti normativi efficaci e basati sul monitoraggio dei rischi. A tal fine l'art. 98 della direttiva "PSD2" ha demandato all'Autorità bancaria europea (EBA) il compito di emanare progetti di norme tecniche di regolamentazione indirizzati ai prestatori di servizi di pagamento, in cui sono specificate anche le misure di sicurezza per tutelare la riservatezza e l'integrità sia delle credenziali di sicurezza personalizzate degli utenti di servizi di pagamento1 che delle operazioni di pagamento eseguite";

- "gli Standard Tecnici di Regolamentazione ("RTS") elaborati dall'EBA, adottati con il Regolamento Delegato (UE) 2018/389 della Commissione, prevedono che i servizi di pagamento offerti elettronicamente dagli intermediari dovrebbero essere prestati in maniera sicura, ricorrendo a tecnologie in grado di garantire l'autenticazione sicura dell'utente e di ridurre il più possibile il rischio di frodi. La procedura di autenticazione dovrebbe includere, in generale, meccanismi di monitoraggio delle operazioni al fine di rilevare i tentativi di utilizzo delle credenziali di sicurezza personalizzate di un utente dei servizi di pagamento che sono state perse, rubate o oggetto di appropriazione indebita e dovrebbe altresì garantire che l'utente dei servizi di pagamento sia l'utente legittimo, che pertanto acconsente al

trasferimento di fondi e all'accesso alle informazioni sul suo conto attraverso un utilizzo normale delle credenziali di sicurezza personalizzate";

- "A questo scopo l'art. 2 degli RTS prevede che tali meccanismi di monitoraggio delle operazioni tengano conto, come minimo, dei seguenti fattori di rischio: a) gli elenchi degli elementi di autenticazione compromessi o rubati; b) l'importo di ciascuna operazione di pagamento; c) gli scenari di frode noti nella prestazione dei servizi di pagamento; d) i segnali della presenza di malware in una qualsiasi delle sessioni della procedura di autenticazione; e) se il dispositivo o il software di accesso sono forniti dal prestatore di servizi di pagamento, un registro dell'utilizzo del dispositivo o del software di accesso forniti all'utente del servizio di pagamento e l'utilizzo anomalo degli stessi";

- "Inoltre, l'art. 18 degli RTS prevede che i medesimi meccanismi di monitoraggio vengano utilizzati dagli intermediari ai fini dell'analisi sull'applicazione dell'autenticazione forte del cliente nei casi di operazioni di pagamento elettronico a distanza che presentano un basso livello di rischio, anche sulla base di un'analisi eseguita in tempo reale e finalizzata a rilevare uno dei seguenti elementi: i) uno schema di spesa o di comportamento anomalo del pagatore; ii) informazioni insolite sull'utilizzo del dispositivo o del software del pagatore a fini di accesso; iii) la presenza di malware in una qualsiasi delle sessioni della procedura di autenticazione; iv) uno scenario di frode noto nella prestazione dei servizi di pagamento; v) localizzazione anomala del pagatore; vi) localizzazione ad alto rischio del beneficiario";

- "La normativa quindi richiede ai PSP di effettuare analisi specifiche, utilizzando sia informazioni in proprio possesso e collegate all'avvio di una sessione o all'esecuzione di una transazione da parte del cliente, sia informazioni tipicamente attestate sul dispositivo che il cliente sta utilizzando, per accertare che tale dispositivo non sia oggetto di uso anomalo, che non vi siano software malevoli che stiano intercettando o modificando le informazioni, che non vi siano anomalie riscontrabili nella localizzazione del dispositivo";

- "Al fine di poter efficacemente ottemperare a tali obblighi normativi, che hanno la finalità di garantire la sicurezza dei servizi di pagamento per il pubblico, si rende necessario raccogliere le informazioni oggetto dell'avviso pubblicato sulle App".

2.2 L'attività ispettiva presso Poste Italiane S.p.a.

Al fine di ottenere ulteriori chiarimenti circa le modalità di funzionamento dell'app BancoPosta e dell'app PostePay, nonché in merito alla conformità dei trattamenti di dati personali per mezzo di esse realizzati, l'Autorità, in data 17/07/2024, ha effettuato un accertamento ispettivo, presso la sede di Poste Italiane s.p.a., ai sensi dell'art. 58, par. 1, lett. a), e) e f), del Regolamento e degli artt. 157 e 158 del Codice, nel corso del quale è stato rilevato quanto di seguito riportato.

In particolare:

- XX, quale responsabile del trattamento, gestisce la piattaforma informatica antifrode con l'ausilio di XX che, in qualità di sub-responsabile, fornisce la componente ThreatMetrix, già integrata nella piattaforma antifrode (PIAF);

- entrambe le app (Bancoposta e PostePay) sono state progettate e sviluppate da Poste Italiane e PostePay, con la collaborazione di XX che, in qualità di responsabile del trattamento, ne cura anche la manutenzione; in questa fase, può accadere che XX, in via incidentale, acceda a dati personali;

- rispetto alla effettuazione della valutazione di impatto ai sensi dell'art. 35 del Regolamento, è stato rappresentato che la stessa è stata effettuata per i diversi trattamenti dei dati personali necessari per le attività antifrode;

- rispetto al funzionamento delle app, in relazione al trattamento che prevede l'accesso ai "dati di utilizzo" presenti sul dispositivo, è stato illustrato che le suddette applicazioni effettuano l'inizializzazione della libreria ThreatMetrix, mediante ID di correlazione generato con Access Token che identifica il cliente. La libreria ThreatMetrix utilizza il suddetto ID, associato alle informazioni estratte dal dispositivo del cliente, per creare il profilo specifico del dispositivo, necessario alle funzionalità di rilevamento delle frodi fornite dalla libreria stessa;

- rispetto alle valutazioni tecniche alla base della soluzione progettuale adottata che prevede l'uso della libreria ThreatMetrix e le considerazioni a supporto di tale preferenza, rispetto ad altre possibili scelte implementative, è stato rappresentato che, tra le possibili soluzioni disponibili sul mercato, Poste Italiane ha deciso di adottare la soluzione offerta da XX, già predisposta all'integrazione con la tecnologia di XX, reputata la più adatta alla realtà di Poste Italiane, sia per una più agevole integrazione con i propri sistemi di Fraud Management (XX), sia per la prevista efficacia, nonché per la reputazione della soluzione che prevede l'utilizzo della libreria ThreatMetrix;

- rispetto alle modalità e alla logica di invocazione delle funzionalità software della libreria ThreatMetrix, ovvero sotto quali condizioni avviene l'accesso ai dati di utilizzo del dispositivo e il relativo invio, mediante le funzionalità di tale libreria, ai sistemi cloud del Responsabile, è stato specificato che la libreria è inizializzata, all'avvio dell'applicazione, generando un ID di correlazione. Successivamente, la libreria stessa recupera le informazioni relative alle app in esecuzione, le associa all'ID e le trasmette al cloud di XX. In seguito a tali operazioni, viene aggiornato il profilo del dispositivo utilizzato dalla libreria ThreatMetrix nelle successive operazioni dispositive. La logica di tale utilizzo viene realizzata internamente alla citata libreria. È stato specificato altresì che, allo stato attuale, l'aggiornamento del profilo avviene solamente in fase di post-login;

- sono state verificate le modalità di inizializzazione della libreria e della creazione del profilo del dispositivo. È stato altresì accertato che l'estrazione dei "dati di utilizzo", relativo alle app in esecuzione, così come i successivi aggiornamenti del profilo del dispositivo, è demandato, alla libreria ThreatMetrix che ne gestisce le modalità e le logiche di accesso;

- è stato altresì effettuato un accesso all'indirizzo www.portal.threatmetrix.eu, esposto su rete pubblica con canale sicuro SSL, con profilo di monitoraggio, alla console "XX", che consente la consultazione delle operazioni effettuate dai clienti, al fine di verificarne il funzionamento e i dati ivi contenuti; nell'ambito delle attività, è stato constatato che l'accesso alla console avviene mediante una procedura di autenticazione informatica a un solo fattore (username/password). Nel corso della verifica all'interno della suddetta console, sono state analizzate le informazioni registrate dalla soluzione di XX, sui propri sistemi, e messi a disposizione degli utenti autorizzati dei titolari del trattamento che effettuano il monitoraggio, mediante esecuzione di specifiche interrogazioni (query) che consentono di recuperare liste di operazioni, caratterizzate da diversi attributi (colonne). È altresì emerso che la console in questione presenta l'attributo "malicious installed apps" che, quando valorizzato, riporta l'elenco delle applicazioni "malevole" installate sul dispositivo, come elenco di stringhe hash MD5 separate da virgole;

- è stato inoltre chiarito che entrambe le app (BancoPosta e PostePay) trattano anche altri dati - tra i quali le informazioni relative alle app installate - e che si trattava di un trattamento già presente al momento dell'introduzione della funzionalità oggetto dell'ispezione;

- con riferimento a questi trattamenti di dati personali, è risultata essere stata predisposta un'apposita informativa, nella quale si legge che "i dati personali che Poste Italiane S.p.A. tratta sono raccolti presso l'interessato (anche presso l'Ufficio Postale), tramite Contact

center o corrispondenza elettronica, oppure, nel corso dei vari rapporti in essere, possono essere ottenuti attraverso altri canali quali, ad esempio: siti web, social network, chat, App (quali ad esempio i dati raccolti dalla rubrica dei contatti del dispositivo per i servizi di ricarica telefonica e P2P, il numero di telefono per la trasmissione ai sistemi anti frode di Poste Italiane per proteggere i tuoi pagamenti) […]. Tali identificativi possono lasciare tracce che, se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate, con il Suo consenso, per creare profili individuali; elenchi pubblici ed elenchi di contraenti ("contraenti" sono coloro che hanno stipulato un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico); altri Titolari/Contitolari del trattamento";

- è stato altresì rappresentato che l'ID dispositivo, gestito dal Responsabile (XX) e generato a partire da un Session Token, è utilizzato solo in ambito di autenticazione e nell'invocazione delle API (Application Programming Interface) interne dei sistemi Poste Italiane e non ha nessuna correlazione con altri identificativi/tracker analitici;

- rispetto alle modalità di trasmissione dei dati al responsabile del trattamento e alle relative misure di sicurezza utilizzate (cfr. cifratura del canale di trasmissione), è stato chiarito che tutte le invocazioni di API, effettuate da entrambe le app, fanno uso di canali cifrati con TLS 1.2 o superiori;

- è stato rappresentato inoltre che i tempi di conservazione (retention) dei dati (le operazioni effettuate, (data, ora e importo della transazione), le informazioni sugli account (da cui spesso sono desumibili nome e cognome dell'utente) e i codici hash delle app malevole individuate (da cui è facilmente ricavabile il nome in chiaro, cfr. par. 5.4), oltre a una serie di altri dati utilizzati per il fingerprinting del dispositivo (sistema operativo e relativa versione, uso di VPN, indirizzo IP, ID ThreatMetrix, ecc.) ammontano a 6 mesi e che le Società per monitorare tali tempi, utilizzano la console "XX" precisando che la stessa non consente di eseguire query con finestra temporale anteriore ai 6 mesi, rispetto al giorno di interrogazione;

- è stato effettuato l'accesso alla console "XX" con la stessa utenza utilizzata precedentemente, al fine di eseguire una query, a partire da dicembre 2023. Così facendo, è stato effettivamente verificato che la console non consente l'esecuzione di query che hanno una finestra temporale di interrogazione con data di inizio precedente ai 6 mesi rispetto al giorno di interrogazione. Nell'ambito dello stesso accesso, è stata anche verificata la presenza di informazioni direttamente riconducibili agli interessati (User ID nella forma nome.cognome);

- è stato, altresì, specificato che, per le versioni delle app installate sul sistema operativo Android fino alla versione 7, tale funzionalità non era implementata, in quanto non supportata dal sistema operativo. Le versioni delle app. sono: app PostePay, dalla release 11.405.9 e app. BP, dalla release 20.336.5.

- è emerso inoltre che il numero di app Android "BancoPosta (BP)" installate dai clienti, al momento dell'accertamento, ammontava a 5.969.456, mentre il numero di app Android "PostePay (PP)" installate dai clienti, al momento dell'accertamento, era pari a 8.596.350 (in entrambi i casi, oltre un milione di app non supportavano la funzionalità oggetto di ispezione);

- è risultato ancora che il numero di app per le quali risultava acquisito il consenso degli interessati era pari a 3.226.938, per BP, e pari a 4.492.040 per PP, mentre n. 108.051 app BP e n. 195.829 app PP risultavano bloccate al momento dell'accertamento, in considerazione del mancato rilascio del consenso da parte dei clienti.

Successivamente, con nota del 05/08/2024, le Società hanno provveduto a sciogliere le riserve avanzate in sede ispettiva, completando la consegna delle informazioni e della documentazione richiesta.

2.3 La seconda richiesta di informazioni ai sensi dell'art. 157 del Codice e le ulteriori integrazioni.

Con nota del 25/11/2024, le Società hanno fornito riscontro a un'ulteriore richiesta di informazioni, formulata dall'Autorità in data 15/10/2024 (prot. n. 119912), rappresentando che:

- "si conferma come l'individuazione di XX quale sub-responsabile sia stata concordata con XX tramite la compilazione dell'Allegato IV ("Elenco dei sub-responsabili del trattamento") al menzionato contratto di nomina";

- "I dati personali (i "Dati") recuperati attraverso l'SDK ThreatMetrix (l'"SDK") sono trattati solo nei sistemi informatici di XX e in PIAF, che è una piattaforma gestita on premises nell'infrastruttura informatica di Poste Italiane. Pertanto, i sistemi che trattano i dati sono:

  • quelli del sub-responsabile del trattamento XX e;

  • la Piattaforma Integrata Anti Frode (PIAF) nell'ambito dei sistemi informatici di Poste Italiane (on premises)";

- "l'intero set di dati recuperato tramite l'SDK ThreatMetrix viene utilizzato dai sistemi XX per fornire alla Piattaforma Integrata Anti-Frode (PIAF) l'esito dell'analisi del rischio compendiato in uno score. La Piattaforma Integrata Anti Frode (PIAF) memorizza solo un subset di questi dati, alcuni dei quali inclusi come indicatori logici di eventi (es. presenza di malware: sì o no). In linea generale, tutti i dati restituiti nella response della chiamata Application Programming Interface - API (sessionQuery) vengono memorizzati in un campo character large object ("CLOB") del database storico di PIAF al solo fine di logging e, rimanendo sempre confinati all'interno di PIAF, non sono consultabili per altri fini. Solo un ristretto subset di tali attributi (12) viene memorizzato nelle tabelle operazionali ed utilizzato per le attività di fraud detection che possono portare, eventualmente, alle attività di approfondimento fino al blocco dell'operazione dispositiva";

- "i dati archiviati all'interno dei sistemi di ThreatMetrix di XX per un periodo di conservazione pari a 24 mesi, fanno riferimento ai dati presenti nel database di Analytics. A seguito dell'individuazione da parte del sub-fornitore XX di un refuso nella documentazione fornita dallo stesso, si rettifica il termine di conservazione del dato, da 24 a 28 mesi. I suddetti dati vengono sottoposti ad "hashing at rest" e non sono decifrabili. Essi vengono distrutti dopo il superamento del Time To Live ("TTL") di 28 mesi. Le motivazioni sottese alla scelta di prevedere un periodo di conservazione pari a 28 mesi all'interno del database Analytics di ThreatMetrix sono di natura analitica e statistica".

Esaminati gli atti, si è quindi ritenuto di richiedere ulteriori elementi di precisazione, cui le Società hanno fornito riscontro, con due note distinte. In particolare, con la comunicazione del 20/1/2025, è stato specificato che:

- "l'elenco dei campi di output, restituibili dalla response e memorizzabili all'interno del campo CLOB, sono stati elencati e presentati nei seguenti documenti uniti alle precedenti interlocuzioni con l'Autorità […]";

- "[…] i dati relativi alle App installate e in esecuzione (ovvero i codici hash delle applicazioni rilevate sul dispositivo) attualmente non vengono restituiti nella response della chiamata API; pertanto, questi ultimi non sono oggetto di trattamento all'interno della Piattaforma Integrata

Anti Frode (PIAF), come indicato dalla colonna service_type “Attribute-Reference-Matrix-Poste-DeviceSecurityHealth_Running v2”;

- “il campo CLOB (così come il subset di attributi) ricevuto da XX è memorizzato in PIAF su archivi Oracle (Oracle Database 19c Enterprise Edition Release presente su macchine on-premises collocate, quindi, all’interno dei Data Center di Poste Italiane) accessibile ai soli utenti autorizzati ed opportunamente profilati ed è un oggetto di tipo BLOB (dato binario non strutturato, non direttamente intellegibile)”.

Successivamente, a seguito d’interlocuzione con il fornitore della soluzione tecnologica (XX), le Società, con nota del 30/01/2025, hanno ulteriormente chiarito che:

- “i dati del dispositivo dell’utente attualmente raccolti durante la fase di profiling dell’utente sono memorizzati nel Profiling Server senza essere associati a un utente specifico. La memorizzazione è temporanea (con time to live di ventiquattro ore). Tali dati sono crittografati sia in transito che a riposo. Durante la fase di profiling, ai dati del dispositivo vengono associati i parametri org_id e session_id, rispettivamente identificativi univoci dell'organizzazione cliente di XX e della sessione applicativa dell’utente finale”;

- “successivamente, nella fase di chiamata API, è possibile il trattamento di dati personali associati a uno specifico utente/interessato tramite la soluzione XX. Anche la trasmissione di questi dati avviene tramite canale crittografato adoperante protocollo TLS 1.2 o superiore. Le relative specifiche sulle tecniche di crittografia e hashing sono quelle in precedenza descritte nel documento “Elementi informativi per il Garante Privacy (XX)”, già agli atti del procedimento. Tramite la chiamata API effettuata dalla Piattaforma Integrata Anti Frode (PIAF), XX riceve contestualmente alle PII anche i parametri org_id, api_key e session_id; dunque, solo dopo la chiamata API risulta possibile associare il dato profilato alle PII dell'utente”;

- “le PII trasmesse dalla Piattaforma Integrata Anti Frode (PIAF) non sono inviate al Profiling Server, ma direttamente all’infrastruttura di backend di XX, come riportato al punto 5. “Misure di Sicurezza” del sopra menzionato documento “Elementi informativi per il Garante Privacy”. Quindi, qualsiasi PII trasmessa dagli utenti alla piattaforma tramite le chiamate API viene trasmessa tramite un canale TLS 1.2 o superiore direttamente ai data center di XX. In fase di archiviazione, tali PII sono cifrate e sottoposte a hash”.

3. L’avvio del procedimento per l’adozione dei provvedimenti correttivi e sanzionatori e le deduzioni delle Società.

All’esito degli approfondimenti istruttori sopra descritti, caratterizzati da una elevata complessità di natura tecnologica (cfr. Relazione tecnica del 20/3/2025) e dell'esame di tutta la documentazione e delle dichiarazioni acquisite in sede istruttoria, l’Ufficio ha rilevato che la soluzione tecnica adottata dalle Società al fine di innalzare il livello di sicurezza informatica nelle transazioni bancarie disposte tramite canali digitali, considerata l’ampiezza e la quantità di informazioni che vengono raccolte, presentava profili di presunta violazione del quadro normativo in materia di protezione dei dati personali per i motivi di seguito analiticamente specificati.

In sintesi, la specifica configurazione dell’applicativo ThreatMetrix appariva eccessivamente invasiva della sfera giuridica dell’interessato, in quanto il pur rilevante obiettivo di innalzare il livello di sicurezza informatica e di operare un maggiore controllo antifrode avrebbe potuto utilmente essere raggiunto dalle Società mediante l’utilizzo di strumenti, eventualmente anche tra loro combinati, meno impattanti sui diritti degli utenti finali.

Di conseguenza, con nota del 2/4/2025, l’Ufficio ha notificato alle Società, contitolari del

trattamento dei dati personali dei clienti effettuato per il tramite delle app Bancoposta e PostePay, l'avvio del procedimento per l'adozione dei provvedimenti di cui agli artt. 58, par. 2, e 83 del Regolamento, in conformità a quanto previsto dall'art. 166, comma 5, del Codice, in relazione alla presunta violazione delle disposizioni di cui agli artt. 5, 6, 13, 25, 28, 32, 35 del Regolamento e dell'art. 122 del Codice in materia di protezione dei dati personali (d.lgs. 196/2003).

In particolare, è stato rilevato che i trattamenti in questione sono stati effettuati, in assenza di una idonea condizione di liceità e senza che sia stata fornita una specifica e adeguata informativa sugli stessi agli interessati; è stata altresì ravvisata la mancanza di misure volte a garantire che tali trattamenti di dati personali fossero conformi ai principi di protezione dei dati, fin dalla progettazione e per impostazione predefinita, tra cui l'effettuazione di una specifica valutazione di impatto preventiva all'utilizzo della soluzione tecnologica prescelta (DPIA), avente lo scopo di rilevare e mitigare i rischi elevati che trattamenti siffatti comportano per i diritti e le libertà degli interessati.

Sono risultate altresì inadeguate le misure di sicurezza apprestate ed è stato rilevato il mancato rispetto del principio di limitazione della conservazione dei dati, nonché degli obblighi in materia di designazione del responsabile del trattamento.

3.1 La memoria difensiva.

Con nota del 30/4/2025, le Società hanno fatto pervenire un'articolata memoria difensiva (corredata di allegati) con la quale, nel formulare richiesta di audizione, hanno rappresentato quanto di seguito riportato.

In merito alla contestata violazione dell'art. 122 del Codice (accesso ai dati relativi alle app in esecuzione o installate sugli smartphone dei clienti, in assenza di un consenso libero, specifico e informato dei clienti stessi), le Parti hanno rappresentato che "la scelta delle Società d'installare ThreatMetrix prescindendo dal consenso degli Interessati è conforme al Codice", in quanto:

> - "Il menzionato art. 122, infatti, esonera dal requisito del consenso preventivo in tutte le ipotesi in cui il trattamento sia svolto "[…] nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio […]". Il trattamento connesso all'uso di ThreatMetrix rientra indubbiamente e pienamente in questa fattispecie. Ciò perché il requisito della 'stretta necessità' non si limita al mero funzionamento delle App, bensì si estende alla garanzia che le App medesime funzionino conformemente alle regole normative e tecniche di riferimento, inclusi i requisiti di sicurezza del servizio. Pertanto, come sopra argomentato, l'uso di ThreatMetrix è strettamente necessario alla fornitura dei servizi tramite le App da parte delle Società, costituendo una concreta attuazione degli obblighi di diligenza professionale cui le Società medesime devono conformare le proprie azioni, oltre che dei doveri derivanti dalle norme cogenti meglio descritte al punto 2.1.2 [della stessa memoria difensiva]";
>
> - "Infatti, gli "Orientamenti 2/2023 sull'ambito di applicazione tecnico dell'articolo 5, paragrafo 3, della direttiva e-privacy" del CEPD (Comitato europeo per la protezione dei dati) richiamano integralmente quanto già statuito dal Gruppo di Lavoro Articolo 29 per la Protezione dei Dati […] nel "Parere 9/2014 sull'applicazione della direttiva 2002/58/CE al device fingerprinting". In particolare, il punto 6.5 di tale parere esplicita come le attività di device fingerprinting (quali sono quelle effettuate tramite ThreatMetrix) realizzate "per uno scopo legato alla sicurezza incentrata sugli utenti" non richiedano il preventivo consenso degli utenti medesimi, trattandosi di tecniche relative alla sicurezza di un servizio esplicitamente richiesto dagli stessi. Né i Dati raccolti tramite ThreatMetrix sono stati mai usati dalle Società per perseguire alcun fine secondario rispetto alla sicurezza dell'Interessato. A quest'ultimo riguardo, in coerenza con quanto raccomandato dal WP29,

l'esclusione dell'uso secondario dei Dati è garantita dal fatto che le Società hanno adottato adeguate misure di sicurezza organizzative e tecniche di segregazione dei Dati medesimi: tali misure consistono nella realizzazione e nell'utilizzo della Piattaforma Integrata Anti Frode ("PIAF"), segregata rispetto agli altri sistemi aziendali ed esclusivamente dedicata alle attività di prevenzione di eventuali frodi;

- "la stessa Autorità, […] nel proprio provvedimento n. 231 del 10 giugno 2021 inerente all'uso di cookie e altri strumenti di tracciamento - strumenti anch'essi soggetti alla disciplina di cui all'art. 122 del Codice – non include i c.d. 'cookie di sicurezza' tra quelli necessitanti il preventivo consenso per la loro installazione. In maniera ancora più inequivoca, nel proprio documento istituzionale "Cookies: profili tecnologici" (rif. Doc-Web 4092169) codesta onorevole Autorità ha chiarito che il "[…] il cookie di sicurezza è un sotto-tipo […]" di "[…] cookie tecnico […]" e quindi rientra nell'ipotesi di esonero dal consenso preventivo. Tali principi, statuiti con riguardo ai cookie di sicurezza, sono applicabili anche a uno strumento del tutto analogo dal punto di vista funzionale qual è ThreatMetrix".

Sul medesimo punto, le Società hanno altresì evidenziato come "Il fatto che l'attuazione di misure di sicurezza proattive volte a prevenire eventuali violazioni dei Dati e/o ipotesi di transazioni non autorizzate costituisca un preciso obbligo giuridico delle Società, non demandabile a una scelta discrezionale degli Interessati e che anzi costituisce elemento essenziale dell'erogazione del servizio, emerge anche dalla normativa nazionale in materia, così come interpretata dalla Corte di Cassazione" (cfr. sentenza n. 3780 del 12 febbraio 2024 Terza sezione civile; ordinanza n. 26916 del 26 novembre 2020 Sesta sezione civile).

Ne deriva che "l'attuazione da parte delle Società della misura di sicurezza proattiva costituita dall'uso di ThreatMetrix è strettamente necessaria all'erogazione dei servizi tramite App. Infatti, in mancanza le Società medesime sarebbero incorse in un'ipotesi di violazione dei parametri di diligenza professionale, rappresentati dall'obbligo di attuare sistemi antifrode in linea con i più elevati standard tecnici disponibili sul mercato.

Secondo le due Società, "diversamente da quanto affermato nella Notifica, nessuna violazione del principio di libertà del consenso è rinvenibile nella vicenda in esame, appunto perché nessun consenso doveva essere richiesto dalle Società, non essendo esso la base giuridica applicabile al trattamento dei Dati. Il fatto che, per potere adoperare le App, agli utenti sia stata richiesta una preventiva e specifica autorizzazione all'uso di ThreatMetrix non va infatti confuso con una richiesta di consenso ai sensi degli artt. 4, n. 11 e 7 del Regolamento. Quella rivolta agli Interessati è stata invece una mera richiesta di autorizzazione tecnica. Più specificamente, per rilevare le informazioni relative alle applicazioni installate e/o in esecuzione nei Dispositivi adoperanti sistema operativo Android ("Android"), cioè le informazioni strettamente necessarie a effettuare l'analisi e la catalogazione delle applicazioni medesime per classi di rischio di esposizione a eventuali malware presenti nei Dispositivi (e più precisamente le applicazioni informatiche in esecuzione sugli stessi), tecnicamente le App necessitano di una specifica autorizzazione dell'Interessato, denominata "Usage Data Access". Tale autorizzazione è richiesta da Android e presuppone una gestione manuale da parte dell'utente, in quanto non è possibile gestire tale richiesta dal menu dei permessi delle applicazioni, e serviva a permettere alle App di chiedere ad Android stesso informazioni sui Dispositivi degli Interessati. Questa ricostruzione tecnica è confermata anche nella Relazione tecnica del Dipartimento Tecnologie Digitali e Sicurezza Informatica allegata alla Notifica, ove si legge che "Il permesso android.permission.PACKAGE_USAGE_STATS, è un'autorizzazione a livello di sistema (systemlevel) Android […] espresso mediante una funzionalità presente in un'apposita sezione ("Accesso speciale") all'interno delle impostazioni del dispositivo, raggiungibile mediante Impostazioni Applicazioni Accesso speciale Accesso dati utilizzo (https://developer.android.com/training/permissions/requesting-special?hl=it) […]". In mancanza di tale autorizzazione tecnica, le Società avrebbero dovuto concedere l'uso delle App senza

un’adeguata protezione anti-malware in favore degli Interessati, modalità che – sulla base di quanto sopra esposto – avrebbe comportato una violazione delle norme cogenti applicabili alle Società – e meglio descritte al successivo punto 2.1.2 [della stessa memoria difensiva] – oltre che dei rilevanti canoni di diligenza professionali”.

Per quanto riguarda la violazione dell’art. 6 del Regolamento, le Società hanno dichiarato che alle stesse “non è ascrivibile alcuna violazione dell’art. 6 del Regolamento, in quanto non solo l’indicazione della base giuridica dell’obbligo normativo in relazione all’uso del sistema di sicurezza ThreatMetrix è connessa alla necessità per le Società di conformarsi alla normativa in materia di sicurezza dei pagamenti, ma l’uso di ThreatMetrix è anche necessario alle Società per adempiere agli obblighi in materia di sicurezza di cui all’art. 32 del Regolamento. Infatti, con particolare e precipuo riguardo al requisito di cui all’art. 2, par. 2, lett. d) del Regolamento Delegato [(UE) 2018/389] – richiamato peraltro anche nel successivo art. 18, par. 2, lett. c), punto iii) del Regolamento Delegato stesso -, il quale impone espressamente alle Società di rilevare e gestire i rischi connessi a “[…] segnali della presenza di malware in una qualsiasi delle sessioni della procedura di autenticazione […], pare chiaro come tale obbligo possa essere adempiuto solo ed esclusivamente tramite un accesso ai Dati presenti nei Dispositivi degli Interessati. D’altro canto, i trattamenti realizzati usando ThreatMetrix consentono alle Società di garantire la sicurezza del trattamento dei Dati degli Interessati, prevenendo eventuali violazioni dei Dati medesimi connesse all’uso delle App e pertanto ThreatMetrix è a tutti gli effetti qualificabile come una delle “[…] misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio […]” alla cui adozione le Società sono tenute a norma dell’art. 32 del Regolamento”.

Del resto, le disposizioni del Regolamento delegato anzi citato impongono “la realizzazione di misure di sicurezza tecnologiche conformi allo stato dell’arte (qual è ThreatMetrix), senza entrare nel dettaglio della specifica tecnologia da adottare: ciò in quanto qualsiasi indicazione normativa puntuale al riguardo sarebbe soggetta a rapida obsolescenza, stante l’incessante avanzare del progresso tecnologico caratterizzante il settore della sicurezza informatica”.

In termini più generali, quindi, “l’adoperabilità della base giuridica di cui all’art. 6, par. 1, lett. c) del Regolamento ha quale prerequisito non già l’esistenza di una descrizione esaustiva del trattamento medesimo contenuta nella norma di riferimento, bensì la mera presenza di una connessione funzionale e teleologica del trattamento rispetto all’obbligo normativo cui il titolare del trattamento stesso è soggetto”.

Le Società hanno peraltro evidenziato come, in relazione alla possibilità di ricorrere alla base giuridica del c.d. “legittimo interesse”, “i riferimenti normativi relativi al concetto di legittimo interesse circoscrivono tale definizione a finalità proprie del titolare del trattamento […]. Cosi non è nel caso in oggetto poiché l’interesse perseguito - consistente nel tutelare la sicurezza dei Dati trattati tramite le App e delle operazioni effettuate attraverso le App medesime, contemporaneamente gestendo i rischi connessi a eventuali frodi di cui gli Interessati potrebbero essere vittime - appartiene esclusivamente e unicamente agli Interessati”; difetterebbe dunque, nella fattispecie in esame, “la caratteristica di alterità tra gli Interessati e la titolarità dell’interesse perseguito, alterità che è invece requisito essenziale per la fruibilità della base giuridica del legittimo interesse”.

Per quanto riguarda invece la violazione degli artt. 5, par. 1, lett. a) e 13 del Regolamento, le Società hanno sottolineato come “non sia [ad esse] ascrivibile alcuna violazione degli artt. 5, par. 1, lett. a) e 13 del Regolamento, poiché [le stesse] hanno fin dall’inizio predisposto delle informative sul trattamento dei Dati inerente alle App contenenti tutti gli elementi richiesti dagli artt. 12 ss. del Regolamento. Altresì, a fronte dei rilievi di codesta onorevole Autorità e senza che ciò possa considerarsi quale assunzione di responsabilità, le Società si sono in ogni caso successivamente attivate procedendo alla revisione delle applicabili informative sul trattamento dei

Dati, onde renderle ulteriormente dettagliate (documento in via di pubblicazione e prodotto in allegato). Più specificamente, con riguardo alle nuove funzionalità di sicurezza delle App, le Società hanno inviato preliminarmente agli Interessati un messaggio tramite cui si è comunicato agli stessi in forma semplice, chiara e diretta come, per garantire un'esperienza sicura di utilizzo delle App medesime, fosse necessaria l'introduzione dei nuovi strumenti di sicurezza sopra menzionati. In tale sede, è stato parimenti chiarito agli Interessati come l'accesso ai Dati di utilizzo dei Dispositivi avvenisse allo scopo di monitorare le applicazioni utilizzate e la relativa frequenza di uso, delineando in forma sintetica, ma precisa e immediata, la finalità del trattamento dei Dati (cioè, rilevare la presenza di eventuali applicativi dannosi e/o malevoli) e i Dati oggetto del trattamento stesso (cioè i Dati di utilizzo inerenti ai Dispositivi). Ancora, tramite tale messaggio le Società hanno informato in modo esplicito, immediato e diretto gli Interessati del fatto che l'attivazione delle nuove funzionalità di sicurezza è imprescindibile per l'uso delle App, comunicando altresì agli stessi la circostanza per cui, in caso di mancata attivazione delle sopra menzionate funzionalità di sicurezza, l'utilizzabilità delle App sarebbe stata inibita, per ovvie ragioni connesse all'impossibilità per le Società di erogare i relativi servizi in maniera conforme alle vigenti norme in materia di sicurezza dei dati e delle operazioni di pagamento, oltre che nel rispetto dei rilevanti canoni di diligenza professionale cui le Società medesime devono aderire".

Con riferimento alla violazione dell'art. 28, par. 1 del Regolamento, le Società hanno rappresentato che "ThreatMetrix non è un applicativo realizzato su misura per le Società, ma una soluzione standard ampiamente diffusa sul mercato e adoperata da svariati operatori del settore bancario, finanziario e dei servizi di pagamento.

Inoltre, viene riferito che "le Società avrebbero dovuto svolgere delle analisi di elevatissima complessità tecnica e fornire istruzioni altamente dettagliate di tipo tecnologico-operativo in merito alla configurazione di ThreatMetrix, senza tenere conto del fatto che trattasi di una soluzione tecnologica caratterizzata da un rilevantissimo grado di complessità tecnologica e fornita da primario operatore di mercato, il quale è tenuto a fornire autonome garanzie in tema di conformità delle proprie soluzioni alle vigenti regole in materia di protezione dei dati personali".

Risulta quindi "sproporzionato imporre alle Società l'obbligo di svolgere una preventiva valutazione tecnica di dettaglio sulle specifiche tecniche di funzionamento di tale applicativo, avendo invece ottenuto le Società solide garanzie documentali di conformità dei responsabili del trattamento coinvolti rispetto ai requisiti di cui al Regolamento già prima dell'avvio del trattamento medesimo".

Le Società sostengono, altresì, che nessuna "particolare rilevanza debba attribuirsi al rilievo temporale inerente all'esistenza di un precedente accordo (risalente al 2022) tra XX e XX: come anticipato, infatti, la soluzione in esame è fornita in modalità standard ed è adoperata da primari operatori nazionali ed esteri; è quindi del tutto normale che le condizioni contrattuali standard di utilizzo proposte dal fornitore indichino già – in via preventiva ed estensiva – l'elenco di tutte le potenziali funzionalità e di tutti i potenziali subfornitori che potrebbero essere coinvolti nell'erogazione dei servizi. Non è immaginabile, in altri termini, che ciascun aspetto del servizio e ciascuna funzionalità delle soluzioni informatiche proposte da XX e XX e di volta in volta attivate e/o richieste dalle Società siano oggetto di specifica e integrale negoziazione, non fosse altro per il fatto che alcuni aspetti di natura eminentemente tecnica delle soluzioni offerte da tali soggetti (non essendo oggetto di una progettazione 'dedicata' alle Società) risultano coperti da vincoli di riservatezza e/o segreto industriale".

Per quanto concerne, invece, l'obbligo di cui all'art. 28, par. 3, del Regolamento, secondo cui i trattamenti posti in essere dal responsabile devono essere specificamente disciplinati da un contratto o da altro atto giuridico che vincoli il responsabile al titolare, le Società contestano che tale contratto debba assicurare "un livello di granularità nella descrizione dell'oggetto […] come quello preteso da codesta onorevole Autorità". Quanto all'ulteriore profilo di contestazione sul punto (errata compilazione dell'all. 4 di cui al contratto di nomina XX), si tratterebbe

semplicemente di “errori materiali senza conseguenze dirette sui diritti degli interessati”.

In ogni caso, la Società, “in ottica di proattiva collaborazione con l’Autorità”, ha provveduto a revisionare “l’accordo per il trattamento dei dati personali sottoscritto con XX, la cui versione aggiornata e sottoscritta tramite scambio di corrispondenza è allegata alla presente nota”.

Con riferimento alla violazione degli artt. 25 e 35 del Regolamento, le Società, nell’osservare che il “principio di responsabilizzazione di cui agli artt. 5, par. 2 e 24 del Regolamento rimette alla discrezionalità del titolare del trattamento l’identificazione dei modi migliori per la gestione dei menzionati adempimenti, la quale pertanto non si basa su criteri generali, predefiniti e univoci”, hanno innanzitutto illustrato le caratteristiche tecniche e organizzative dell’applicativo ThreatMetrix che, secondo le Società, assicurerebbe la “conformità ai requisiti di cui all’art. 25 del Regolamento”; quindi hanno precisato che “adottare una soluzione di protezione non reattiva ma proattiva, che anticipa esigenze future in maniera dinamica, consente alle Società di prevenire il consolidamento di scenari di frode diffusi, evitando così di dovere intervenire successivamente con misure di contrasto che potrebbero risultare lente e inefficaci. In assenza di questi presidi, si produrrebbe un danno a carico degli Interessati, con potenziali ripercussioni economiche e legali. Investire in tecnologie all’avanguardia per la sicurezza, come ThreatMetrix, offre la possibilità d’identificare tempestivamente attività sospette e bloccare eventuali attacchi prima che possano avere un impatto significativo”.

In particolare, l’“approccio proattivo adottato dalle Società è del resto in linea anche con le recenti indicazioni espresse dall’Autorità Bancaria Europea (“ABE”)” di talché “ne consegue [che] l’adozione di ThreatMetrix, accompagnata dalla previsione della sospensione preventiva dell’operatività tramite le App in assenza dell’attivazione di tale componente anti-malware, sia una condotta pienamente conforme al principio di responsabilizzazione e più in generale alle disposizioni del Regolamento, nel contesto evolutivo della lotta alle frodi, nonché coerente con le finalità della regolamentazione tecnica di riferimento e con gli orientamenti giurisprudenziali in materia”. […]

Le parti hanno inoltre sostenuto che le misure della pseudonomizzazione e minimizzazione messe in campo dalle Società escluderebbero, in radice, la violazione dell’art. 25 del Regolamento, poiché, peraltro, tali misure “hanno contribuito a escludere sin dall’origine la presenza di un potenziale rischio elevato per i diritti e le libertà delle persone fisiche e il conseguente obbligo di effettuare una valutazione d’impatto sulla protezione dei dati a norma dell’art. 35 del Regolamento”; le stesse avrebbero altresì comportato “effetti positivi in termini di riduzione del rischio per i diritti e le libertà delle persone fisiche”, in linea con quanto stabilito dalle “Guidelines 01/2025 on Pseudonymisation” e le recenti pronunce giurisprudenziali della Corte di Giustizia dell’Unione Europea (sentenza del 26 aprile 2023 nella causa T-557/20 – Comitato di Risoluzione Unico (CRU) contro Garante Europeo della Protezione dei Dati (GEPD); nello stesso senso, peraltro, vanno le conclusioni dell’Avvocato Generale della CGUE nella relativa causa di appello C-413/23 P).

In merito al rispetto degli obblighi di cui all’art. 35 del Regolamento, le Società nel ribadire “come la “[…] valutazione di impatto ai sensi dell’art. 35 del Regolamento […] è stata effettuata per i diversi trattamenti dei dati personali necessari per le attività antifrode […]”, hanno contestato l’ “automatismo secondo cui il mancato svolgimento della DPIA determina automaticamente la violazione dell’art. 25 del Regolamento in materia di protezione dei dati fin dalla progettazione e per impostazione predefinita. Tale automatismo non trova tuttavia riscontro in numerosi altri provvedimenti di codesta onorevole Autorità che, pur sanzionando alcuni titolari del trattamento per violazione dell’art. 35 del Regolamento, non ha contestato agli stessi il mancato rispetto dell’art. 25 del Regolamento medesimo (sul punto si vedano, tra gli altri, i provvedimenti nn. 416 del 15 dicembre 2022, 253 dell’8 giugno 2023, 578 del 16 novembre 2023)”.

Infine, le Società hanno dichiarato di aver in ogni caso predisposto “una versione aggiornata e più dettagliata della DPIA inerente all’uso di ThreatMetrix” (all. sub 5 alla memoria difensiva).

Per quanto riguarda la contestazione relativa al periodo di conservazione dei dati (art. 5 par. 1, lett. e) del Regolamento, le Società hanno evidenziato come il “presunto disallineamento tra il periodo di conservazione dei Dati inizialmente dichiarato a codesta onorevole Autorità e quello effettivo è di entità minima, pari solo a quattro mesi, e comunque motivato sulla base di gestire gli effetti della stagionalità nel contesto dell’analisi di potenziali frodi”.

Inoltre, “non solo la proroga del periodo di conservazione ha avuto durata limitata, ma le attività analitiche e statistiche connesse a tale proroga hanno comunque riguardato Dati crittografati e pseudonimizzati e quindi non riconducibili direttamente e immediatamente agli Interessati - se non addirittura Dati anonimi […]”.

Con riferimento alla violazione dell’art. 32 del Regolamento, le Società, nell'evidenziare di essere “dotate di uno strutturato sistema di gestione della sicurezza dei dati personali, conforme non solo al menzionato art. 32 e alle altre norme cogenti in materia, ma anche alle migliori prassi di riferimento del settore […] [tra cui] a solo titolo esemplificativo […] certificazioni di conformità [a diversi standard ISO/IEC]”, hanno “manifesta[to] il loro impegno pro-futuro a tenere in considerazione le osservazioni (dell’Autorità) in ottica di miglioramento e rafforzamento della propria postura di sicurezza del trattamento […]. [OMISSIS]

Infine, le Società, nel sottolineare come la vicenda esaminata dall’Autorità abbia riguardato solo una parte dei rispettivi clienti, hanno sostenuto che le violazioni contestate debbono essere “qualificate come trascurabili” atteso che agli interessati a cui è stato inibito l’uso dell’app era comunque consentito di usufruire di un canale alternativo di accesso ai servizi ovvero tramite browser; inoltre, le Società si siano immediatamente attivate, nei confronti dei clienti che hanno segnalato il disservizio, fornendo agli stessi chiarimenti circa il funzionamento delle “funzionalità di sicurezza delle App”.

3.2 L’audizione delle Parti.

Durante l’audizione del 4 giugno 2025, Bancoposta e PostePay hanno ribadito che operano in un contesto finanziario altamente regolamentato e dotato di strutture di compliance, con la vigilanza e cooperazione della Banca d’Italia, anche per l’applicazione della normativa PSD2.

Le società hanno contestato il provvedimento dell’Autorità Garante della Concorrenza e del Mercato (AGCM), sostenendo che non abbia adeguatamente considerato il parere della Banca d’Italia, secondo cui, per propri profili di competenza, il sistema anti-malware adottato è coerente con la normativa sulla prevenzione delle frodi avendo comunque le società assicurato la continuità del servizio anche ai clienti che hanno negato l’accesso ai dati.

È stata inoltre contestata la qualificazione dell’attività come pratica commerciale scorretta: secondo le società, l’uso del software ThreatMetrix ha finalità esclusivamente antifrode e non commerciali o promozionali, poiché serve a bloccare transazioni potenzialmente fraudolente.

Le società hanno evidenziato l’aumento dei tentativi di frode informatica (circa 500 milioni di euro nel 2024, il doppio rispetto al 2023) e la crescente sofisticazione degli attacchi, spesso realizzati tramite tecniche di social engineering e malware installati sui dispositivi degli utenti. Le società hanno, inoltre, sostenuto che il sistema adottato consente di individuare tali minacce limitandosi a controllare l’hash delle applicazioni malevole installate sui dispositivi, senza effettuare il trattamento delle relative denominazioni “in chiaro” delle stesse.

Poste ha altresì sottolineato il proprio impegno nella sicurezza dei dati, la revisione dell’informativa privacy e l’aggiornamento della valutazione d’impatto, sostenendo che eventuali criticità rilevate

dal Garante siano solo disallineamenti formali senza conseguenze significative per gli utenti. È stata anche predisposta una valutazione del legittimo interesse (LIA) già nel 2021 a supporto dei processi antifrode.

Infine, le società hanno chiesto che la loro collaborazione con l'Autorità, l'assenza di finalità commerciali e l'incertezza giuridica sulla base normativa siano considerate circostanze attenuanti in caso di eventuali sanzioni, proponendo anche campagne di comunicazione per sensibilizzare gli utenti sulla protezione dei dati e la prevenzione delle frodi informatiche.

4. Il quadro normativo applicabile.

4.1. La natura personale dei dati trattati

Ai sensi dell'art. 4 del Regolamento, per "dato personale" si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

Il medesimo articolo 4, n. 5, del Regolamento, definisce come "pseudonimizzazione" "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

In proposito, occorre osservare che la natura personale del dato non è necessariamente legata alla presenza di specifici elementi al suo interno (i cosiddetti "identificativi diretti", quali il nome e il cognome, la data di nascita, e così via), né alla loro intellegibilità.

La giurisprudenza ha ormai, da molti anni, accolto l'interpretazione secondo la quale un dato è personale se consente di distinguere un individuo, da un altro, all'interno di un gruppo (si veda al riguardo il Parere 4/2007 sul concetto di dati personali adottato dal Gruppo Articolo 29 (WP 29), il 20 giugno 2007 - WP 136), indipendentemente dall'elemento impiegato per effettuare tale distinzione.

Inoltre, deve rilevarsi che il trattamento di pseudonimizzazione (che si distingue dal processo di anonimizzazione che persegue obiettivi tutt'affatto diversi) prevede sempre l'utilizzo di una componente (l'informazione aggiuntiva), conservata separatamente rispetto al risultato del trattamento (il c.d. pseudonimo) che, in combinazione con quest'ultimo, rende il dato personale, in quanto attribuibile a una specifica persona fisica identificata o identificabile.

Questa è peraltro l'interpretazione del concetto di pseudonimizzazione che emerge anche dalla sentenza Breyer (C-582/14) della Corte di Giustizia dell'Unione Europea che, tra le altre cose, sancisce che, qualora sussistano dei mezzi giuridici che consentano a un soggetto di combinare uno pseudonimo con le informazioni aggiuntive (anche se detenute da un terzo), tale combinazione equivale a una identificazione e dunque costituisce un trattamento di dati personali.

Tutto ciò premesso, in relazione all'utilizzo dell'applicativo ThreatMetrix per finalità antifrode, emerge che il monitoraggio delle app costituisce, a tutti gli effetti, un trattamento di dati di natura personale, suscettibile di indicare abitudini di vita dell'individuo, anche con riguardo ad aspetti di natura "sensibile".

Infatti l'elenco delle app, installate o in esecuzione nel dispositivo, può rivelare, tra l'altro, interessi

(sport, giochi, hobby), condizioni di salute (app mediche), orientamento religioso, politico o sessuali (app di culto, partiti, associazioni, di incontri), situazione economica (app di credito, prestiti, trading), abitudini quotidiane (fitness, mobilità, alimentazione).

4.2. La base giuridica del trattamento.

L'art. 6, par. 1 del Regolamento stabilisce che il trattamento dei dati personali "è lecito solo se e nella misura in cui ricorre almeno una delle condizioni" indicate nelle lettere da a) a f), tra cui il consenso espresso dell'interessato, in relazione a una o più specifiche finalità (lett. a), l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento (lett. c) o anche il perseguimento del legittimo interesse del titolare del trattamento o di terzi, "a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali "(lett. f)).

Secondo la disciplina posta dal Regolamento, un trattamento di dati personali può considerarsi lecito, se l'interessato può ragionevolmente prevederlo, sulla base del contesto e delle informazioni ricevute. Il considerando 41 del Regolamento recita infatti "Qualora il presente regolamento faccia riferimento a una base giuridica o a una misura legislativa, ciò non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento, fatte salve le prescrizioni dell'ordinamento costituzionale dello Stato membro interessato. Tuttavia, tale base giuridica o misura legislativa dovrebbe essere chiara e precisa, e la sua applicazione prevedibile, per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia dell'Unione europea (la «Corte di giustizia») e della Corte europea dei diritti dell'uomo."

In ordine al presupposto di liceità di cui alla lett. c), il Considerando 45 del Regolamento prevede che "E' opportuno che il trattamento effettuato in conformità a un obbligo legale al quale il titolare del trattamento è soggetto […] sia basato sul diritto dell'Unione o di uno Stato membro. […] Un atto legislativo può essere sufficiente come base per più trattamenti effettuati conformemente a un obbligo giuridico cui è soggetto il titolare del trattamento […]" e "potrebbe precisare le condizioni generali del presente regolamento che presiedono alla liceità del trattamento dei dati personali, prevedere le specificazioni per stabilire il titolare del trattamento, il tipo di dati personali oggetto del trattamento, gli interessati […], le limitazioni delle finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto" (analogamente anche art. 6, par 3 del Regolamento).

Deve rammentarsi inoltre il Considerando 47 del Regolamento, laddove sancisce che "i legittimi interessi di un titolare del trattamento o di terzi possono costituire una base giuridica del trattamento a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. […] In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine".

Il medesimo Considerando 47 aggiunge altresì che "Costituisce parimenti legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di prevenzione delle frodi".

Vi sono poi trattamenti di dati personali che rientrano nell'ambito di applicazione della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (c.d. Direttiva ePrivacy).

In particolare, l'art. 5, par. 3 dell'anzidetta Direttiva stabilisce che gli Stati membri debbano

assicurare che “l’uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell’apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l´abbonato o l´utente interessato sia stato informato in modo chiaro e completo, tra l´altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento. Ciò non impedisce l’eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente”.

L’art. 122 del Codice, in attuazione della citata Direttiva, dispone che: “L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con modalità semplificate. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio. […]”.

Il comma 2 del predetto articolo prevede inoltre che “Ai fini dell'espressione del consenso di cui al comma 1, possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente”.

Infine, il comma 2-bis. dell’art. 122 dispone che “Salvo quanto previsto dal comma 1, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente”.

4.3. Informazioni da rendere all’interessato

I dati personali devono essere “trattati in modo lecito, corretto e trasparente nei confronti dell’interessato (“liceità, correttezza e trasparenza”)” (art. 5, par. 1, lettere a) del Regolamento).

In particolare, il principio di trasparenza, meglio declinato nell’art. 13 del Regolamento, si traduce nell’obbligo, da parte del titolare del trattamento, di fornire all’interessato tutte le informazioni inerenti al trattamento dei dati personali che lo riguardano, in modo accessibile e comprensibile, rendendolo consapevole, nel momento i cui i dati personali sono ottenuti, anche delle finalità e delle modalità del trattamento e della base giuridica dello stesso, nonché di tutte le ulteriori informazioni necessarie per garantire che il trattamento sia corretto e trasparente (art. 13, par. 1 e 2 del Regolamento).

L’informativa sul trattamento dei dati ha la funzione di realizzare il principio di trasparenza e rende effettivo il controllo dell’interessato sui propri dati.

4.4. La designazione del responsabile del trattamento

L’art. 28, par. 1 del Regolamento dispone che “Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato”. Inoltre, “I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati

personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento".

Il medesimo articolo, al par. 3, stabilisce altresì che "I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico […] che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento […]".

4.5. La valutazione d'impatto.

L'art. 35, par. 1 del Regolamento prevede che "Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".

L'obbligo per i titolari del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati, quando prevista, va inteso nel contesto dell'obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi presentati dal trattamento di dati personali.

4.6. Le misure di sicurezza

I dati personali devono essere "trattati in maniera da garantire un'adeguata sicurezza" degli stessi, "compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" (art. 5, par. f) del Regolamento)

Più specificamente, l'art. 32 del Regolamento dispone che "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, […] "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" (art. 32, par. 1).

Il medesimo articolo prevede altresì che "Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati" (art. 32, par. 2 del Regolamento).

4.7. I tempi di conservazione

Infine, in virtù del principio di limitazione della conservazione di cui all'art. 5, par.1, lett. e), i dati devono essere "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; […]".

L'attuazione del principio di limitazione della conservazione non rappresenta soltanto un adempimento organizzativo: costituisce una tutela sostanziale per la persona. La protezione implicita che ne deriva riguarda la riduzione delle superfici di attacco, la limitazione delle possibilità di accesso non autorizzato ai dati e, di conseguenza, la mitigazione degli effetti potenziali di eventuali violazioni.

5. L’esito dell’istruttoria e del procedimento per l’adozione dei provvedimenti correttivi e sanzionatori.

All’esito dell’esame delle dichiarazioni rese all’Autorità nel corso del procedimento nonché della documentazione acquisita, risulta che Poste Italiane S.p.a. e Postepay S.p.a., in qualità di contitolari, hanno posto in essere trattamenti di dati personali dei clienti, per il tramite delle app Bancoposta e Postepay, che risultano non conformi alla disciplina in materia di protezione dei dati personali per i motivi di seguito analiticamente indicati.

In proposito, si evidenzia preliminarmente che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice “Falsità nelle dichiarazioni al Garante e interruzione dell’esecuzione dei compiti o dell’esercizio dei poteri del Garante”.

5.1 Erronea individuazione della base giuridica.

Nel corso dell’istruttoria, è emerso che le Società hanno individuato la condizione di liceità del trattamento dei dati personali, posto in essere tramite l’applicativo ThreatMetrix, nel necessario adempimento a un obbligo legale (art. 6, par. 1, lett. c) del Regolamento) (v. par. 5.1.2).

Al riguardo, l’Autorità, sulla base degli approfondimenti effettuati, ha tuttavia rilevato - in via preliminare - che, ai fini della corretta individuazione della base giuridica dei trattamenti in questione, è necessario operare una distinzione tra due tipologie di trattamento a cui corrispondono quadri giuridici di riferimento diversi.

In particolare occorre distinguere:

- il trattamento dei dati personali, effettuato dalle Società nella fase di raccolta delle informazioni archiviate nei dispositivi (terminali) in uso agli utenti, il cui quadro giuridico di riferimento è la lex specialis di cui alla c.d. Direttiva e-Privacy;

- i trattamenti successivi posti in essere dalle Società e dal sub-responsabile, relativamente alla rilevazione delle app in esecuzione o, comunque, installate sui dispositivi degli utenti, per finalità antifrode, i quali, invece, rientrano, a pieno titolo, nell’ambito di applicazione della normativa di cui al Regolamento.

5.1.1 Il trattamento dei dati personali che comporta l’accesso a informazioni già archiviate nel terminale dell’utente e la violazione dell’art. 122 del Codice.

Come anzidetto, il trattamento dei dati personali che comporta l’accesso a informazioni già archiviate nel terminale dell’utente trova la sua disciplina specifica nella Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (c.d. Direttiva e-Privacy) (v. sopra, art. 5, par. 3 della Direttiva).

L’art. 122, comma 1 del Codice, che recepisce le previsioni dell’art. 5, par. 3 dell’anzi citata Direttiva, consente il trattamento, senza consenso dell'interessato, esclusivamente “nella misura strettamente necessaria” per l’erogazione di un servizio, espressamente richiesto dall’utente.

Tale previsione introduce dunque un’eccezione, di stretta interpretazione, applicabile unicamente alle operazioni indispensabili al funzionamento tecnico del servizio richiesto e non estendibile a trattamenti ulteriori che, pur risultando funzionali a esigenze di ottimizzazione o riconducibili a finalità di sicurezza o prevenzione delle frodi, non risultino comunque strettamente necessari (e inscindibilmente connessi) all’erogazione del servizio espressamente richiesto, anche tenendo

conto delle ipotesi di esonero dall'obbligo di consenso, individuate dal Gruppo di lavoro ex art. 29 nel Parere n. 9/2014 sull'applicazione della Direttiva 2002/58/CE al device fingerprinting (al riguardo si rinvia alle considerazioni che seguono).

A tal proposito, secondo quanto sostenuto dalle Parti, la raccolta dei dati contenuti nei dispositivi mobili degli interessati e, in particolare, i dati relativi all'elenco delle app installate e in esecuzione su tali dispositivi, sarebbe esonerata dal consenso preventivo degli interessati, così come previsto dall'art. 122 del Codice, in quanto il trattamento è svolto "[…] nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio […]", rapportando tale "stretta necessità" alla conformità delle regole normative e tecniche di riferimento, incluse i requisiti di sicurezza del servizio.

Al riguardo, si rileva però come l'ampiezza delle diverse tipologie di dati raccolti dalla libreria, emersa dalle verifiche effettuate in fase istruttoria e ispettiva, risulta essere eccessiva e sicuramente non "strettamente" necessaria all'erogazione del servizio.

Se, infatti, è indubbio che all'aumentare delle informazioni raccolte — che, nel caso di specie, comprendono alcuni dati tecnici relativi al dispositivo e al suo stato di funzionamento (c.d. device attestation), la tipologia di connessione utilizzata, elementi idonei alla geolocalizzazione, identificativi dell'utente o del dispositivo, nonché informazioni sulla profilazione delle transazioni per finalità antifrode, sino a includere dati strettamente afferenti alla sfera personale dell'utilizzatore, quali l'elenco delle applicazioni installate o in esecuzione — corrisponda generalmente una rappresentazione più precisa e attendibile dell'integrità del dispositivo, del suo effettivo utilizzatore e di eventuali attività malevole in corso, è altrettanto necessario evidenziare che tale raccolta deve comunque rispettare il principio di minimizzazione di cui all'articolo 5, paragrafo 1, lettera c), del Regolamento.

L'obbligo generale di adottare misure di sicurezza non legittima, di per sé, una raccolta di dati personali più ampia di quanto strettamente necessario al perseguimento delle finalità dichiarate.

Laddove, infatti, esistano strumenti e soluzioni tecniche idonee a garantire un livello di sicurezza equivalente che non prevedono (o lo prevedono in misura minore) l'accesso a dati personali o, come nel caso in esame, a informazioni registrate sul dispositivo, deve infatti essere privilegiata la soluzione meno invasiva.

In relazione al caso oggetto della presente istruttoria si evidenzia, infatti, come ThreatMetrix metta a disposizione delle società che utilizzano il servizio una soluzione modulare e configurabile nei servizi e nei dati trattati.

Tale soluzione prevede, nella sua configurazione base, l'accesso a un ampio set di "attributi" tecnici del dispositivo (inerenti al sistema operativo, alle caratteristiche hardware, all'eventuale utilizzo di VPN e proxy, agli indirizzi IP, alla rete cellulare utilizzata e a molti altre) e a diversi identificativi utente/dispositivo (ThreatMetrix ExactID, ThreatMetrix SmartID, Google Advertising ID, Session ID) che consentono di effettuare il "fingerprinting" dello stesso.

Si rileva, inoltre, come le Società contitolari del trattamento, allo scopo di innalzare ulteriormente il livello di sicurezza complessivo, abbiano, a un certo punto, deciso di aggiungere, a tale configurazione base un modulo software "opzionale" (XX) che, attraverso il recupero e l'utilizzo delle informazioni relative alle app installate e in esecuzione (elenco delle firme hash MD5 delle app e i relativi metadati) sui dispositivi degli utenti finali, fornisce una funzionalità di "malware detection".

Tanto considerato, la pretesa "indispensabilità" dell'uso della sopra-descritta configurazione della soluzione ThreatMetrix (e non l'utilizzo del prodotto in sé) appare discendere più da una scelta di

natura organizzativa che giuridica o tecnica: l'innalzamento del livello di sicurezza informatica e del controllo sul rischio frodi può, infatti, essere raggiunto anche mediante l'utilizzo, eventualmente anche combinato, di altri meccanismi con efficacia complessiva paragonabile, ma meno invasivi della sfera strettamente privata dell'utente finale.

Infatti, meccanismi quali ad esempio l'autenticazione multi-fattore (SCA step-up autorizzativi), algoritmi di scoring anonimi, monitoraggi di rete, controlli runtime (RASP), schermate informative specifiche, visualizzate all'interno dell'applicazione durante la convalida di un pagamento per aumentare la consapevolezza dell'utente (c.d. pop-up), sono ampiamente utilizzati, anche da altri operatori del medesimo settore, consentendo l'impiego di un insieme più limitato di attributi mediante l'adozione di una diversa configurazione della medesima soluzione attualmente utilizzata (ThreatMetrix), caratterizzata da un minore grado di invasività e coerente con il principio di minimizzazione sopra richiamato.

Lo stesso fatto che le Società abbiano successivamente provveduto alla disabilitazione della nuova funzionalità e al ripristino del precedente funzionamento, senza particolari disfunzioni, conferma ulteriormente che il ricorso a tali dati non risponde a un requisito di stretta necessità e che la soluzione adottata non può ritenersi pertanto tecnicamente irrinunciabile; ciò, anche alla luce di quanto emerso nel corso dell'istruttoria dell'AGCM, ove le parti hanno espressamente dichiarato che "all'utilizzo del nuovo sistema non è corrisposto, nei primi sette mesi di attuazione, una rilevazione maggiore o più efficiente di fenomeni fraudolenti" (cfr. Provvedimento AGCM n. 31566/2025 del 20 maggio 2025).

In conclusione, la scelta, operata dalle Società, di adottare una soluzione di tracciamento generalizzato su dati personali - la lista delle applicazioni installate o in esecuzione, potenzialmente idonee a rivelare abitudini, interessi, condizioni sanitarie, convincimenti religiosi e altri aspetti potenzialmente rientranti nelle categorie particolari di dati di cui all'art. 9 GDPR - così come la sopra descritta configurazione del prodotto ThreatMetrix risponde dunque più a una strategia volontaria di gestione del rischio che a un effettivo obbligo normativo, poiché la disciplina antifrode richiamata (PSD2) non impone, di per sé, la necessità dei trattamenti di dati personali concretamente effettuati. (vedi infra par. 5.1.2).

Pertanto, la combinazione tra (i) l'elevata intrusività nell'ambito della sfera personale dell'utente, derivante dal trattamento delle informazioni relative alle app installate e in esecuzione sul dispositivo, (ii) l'assenza del requisito della stretta necessità, unitamente alla possibilità di ricorrere a soluzioni tecniche alternative, e (iii) la limitata efficacia dimostrata dalla specifica configurazione della soluzione antifrode adottata, determina l'inapplicabilità dell'esonero dall'obbligo di acquisizione del consenso preventivo degli interessati, previsto dall'art. 122 del Codice, così come prospettato dalle Parti, e configura non solo una violazione del principio di minimizzazione di cui all'art. 5, par. 1, lett. c) del Regolamento, ma integra altresì una violazione del principio di protezione dei dati fin dalla progettazione e per impostazione predefinita, sancito dall'art. 25 del GDPR, come ribadito dall'EDPB nelle pertinenti linee guida (cfr. par. 5.4).

Sullo stesso punto, le Società sostengono, inoltre, che "le attività di device fingerprinting (quali sono quelle effettuate tramite ThreatMetrix) realizzate "[…] per uno scopo legato alla sicurezza incentrata sugli utenti […]" non richiedano il preventivo consenso degli utenti medesimi, trattandosi di tecniche relative alla sicurezza di un servizio esplicitamente richiesto dagli stessi", secondo quanto statuito dal Gruppo di Lavoro Articolo 29 per la Protezione dei Dati (Working Party 29 – "WP29") nel "Parere 9/2014 sull'applicazione della direttiva 2002/58/CE al device fingerprinting" richiamato all'interno degli "Orientamenti 2/2023 sull'ambito di applicazione tecnico dell'articolo 5, paragrafo 3, della direttiva e-privacy" Comitato Europeo per la Protezione dei Dati (il "CEPD").

Al riguardo, si rileva preliminarmente che il Parere n. 9/2014 definisce (riprendendo la definizione della RFC69739 dell'Internet Engineering Task Force (IETF)) il fingerprint ("impronta") di un

dispositivo come "una serie di informazioni che identificano un dispositivo o un'istanza applicativa […] in un senso ampio ovvero includendo un insieme di informazioni che possono essere usate per individuare, correlare o dedurre un utente, un programma utente (user agent) o un dispositivo nel tempo".

In sostanza, si tratta di un meccanismo per tracciare un utente (o un dispositivo), non tramite i tradizionali cookie (o procedure di autenticazione), ma usando caratteristiche tecniche o "osservabili" del dispositivo/browser stesso.

Nello stesso parere, sono enumerate quelle che, comunemente, risultano essere le categorie di informazioni (caratteristiche) "tecniche", relative al dispositivo, a cui ci si riferisce per effettuare l'operazione di fingerprinting.

Quando combinate, queste informazioni - seppur di per sé non necessariamente "personali" - costituiscono un'"impronta" sufficientemente univoca o rara al punto tale da consentire di distinguere un dispositivo (o un individuo che ne sia utilizzatore) da quasi tutti gli altri.

Il valore del fingerprint deriva proprio da questa combinazione: mentre una singola caratteristica o parametro tecnico (es. risoluzione dello schermo, sistema operativo utilizzato, stato della batteria, modello del dispositivo) può essere comune a molti utenti, l'insieme combinato di decine (o centinaia) di parametri rende l'impronta rilevata molto più precisa, consentendo così di individuare (tracciare) il dispositivo/utente all'interno dell'insieme considerato.

Un'analoga definizione è riportata, anche da questa Autorità, nelle proprie "Linee guida cookie e altri strumenti di tracciamento" (Provvedimento del Garante n. 231 del 10 giugno 2021), che definiscono il fingerprinting "[…] quella tecnica che permette di identificare il dispositivo utilizzato dall'utente tramite la raccolta di tutte o alcune delle informazioni relative alla specifica configurazione del dispositivo stesso adottata dall'interessato […]".

Anche l'autorità francese Commission Nationale de l'Informatique et des Libertés (CNIL) all'interno delle proprie "Recommendation on mobile applications" definisce il fingerprinting come una modalità di tracciamento, effettuata mediante un identificatore calcolato a partire dalle informazioni tecniche del dispositivo ("Tracking via an identifier calculated from the technical information of the terminal").

Dalle definizioni sopra riportate, risulta evidente come l'elenco delle app installate e/o in esecuzione non può essere annoverato, in generale, tra le "caratteristiche tecniche" di un dispositivo, quanto piuttosto costituisce un dato personale la cui rilevazione è altamente intrusiva, oltreché non strettamente necessaria alla generazione dell'impronta stessa.

Infatti, a differenza di tali caratteristiche tecniche tipicamente utilizzate per il device fingerprinting — quali, ad esempio, il modello del dispositivo, la versione del sistema operativo, la risoluzione dello schermo, la tipologia e la configurazione della connessione o altre proprietà hardware e software generali — l'elenco delle applicazioni installate o in esecuzione può infatti rivelare indirettamente informazioni relative alla sfera personale dell'utente.

A titolo esemplificativo: la presenza di applicazioni dedicate al monitoraggio di specifiche condizioni mediche potrebbe rivelare informazioni relative allo stato di salute dell'utente; la presenza di applicazioni riconducibili a determinate organizzazioni religiose o politiche potrebbe consentire di inferire convinzioni religiose o orientamenti politici; applicazioni relative a incontri o relazioni personali potrebbero suggerire aspetti della vita privata o dell'orientamento affettivo; applicazioni utilizzate per il trading finanziario, il gioco d'azzardo o servizi di prestito potrebbero fornire indicazioni sulle abitudini economiche o sulla situazione finanziaria dell'utente; applicazioni volte alla protezione da minacce informatiche o alla protezione delle comunicazioni (quali app

antivirus e antimalware, app per connessioni VPN) possono infine rivelare la complessiva postura di sicurezza dell'utente del dispositivo.

In tali casi, l'accesso all'elenco delle applicazioni installate o in esecuzione non si limita quindi a descrivere caratteristiche tecniche "neutre" del dispositivo, ma può consentire la deduzione di informazioni relative alla persona che lo utilizza. Per questa ragione, tale informazione deve essere considerata, a tutti gli effetti, un dato personale e, in molti casi, un dato potenzialmente idoneo a rivelare anche categorie particolari di dati, ai sensi della normativa in materia di protezione dei dati personali.

A ulteriore conferma di quanto sopra evidenziato, come già precedentemente riportato, dalla documentazione prodotta nel corso dell'istruttoria e dagli ulteriori approfondimenti effettuati, emerge infatti che il prodotto ThreatMetrix, nella sua configurazione base, - senza l'utilizzo del sopracitato modulo "opzionale" XX – consente già di generare, con soddisfacente precisione, proprio il fingerprint dei dispositivi, mediante la raccolta e l'utilizzo di un ampio set di informazioni tecniche relative agli stessi.

Ne consegue, quindi, che la raccolta della lista delle app installate o in esecuzione, indipendentemente dall'ambito di applicazione e a maggior ragione nel contesto in esame, non rappresenta sicuramente un'informazione meramente tecnica, ma un trattamento di dati personali, non strettamente indispensabile, alla generazione dell'impronta del dispositivo e al suo efficace trattamento, visto, come detto, che la configurazione base di ThreatMetrix, indicata dallo stesso produttore proprio come soluzione idonea al fingerprinting dei dispositivi, non richiede, per il suo funzionamento, l'utilizzo del modulo "opzionale" XX, proposto dallo stesso come specifica soluzione anti-malware.

È stato altresì sostenuto dalle Parti che l'utilizzo della soluzione ThreatMetrix, nella configurazione oggetto della presente istruttoria, sarebbe assimilabile ai c.d. 'cookie di sicurezza', un sotto-tipo di cookie tecnici, così come definiti nel già citato provvedimento di questa Autorità, n. 231 del 10 giugno 2021, inerente all'uso di cookie e altri strumenti di tracciamento e che, per tale motivo, dovrebbero rientrare, per analogia, nell'ipotesi di esonero dal consenso preventivo.

A tal riguardo, si evidenzia che, nello stesso provvedimento, è introdotta una classificazione dei cookie (tecnici e di profilazione) precisando comunque "che [essa] risponde alla ratio della disciplina di legge e dunque anche alle esigenze di tutela della persona […]", e che i cookie tecnici sono "[…] utilizzati al solo fine di 'effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio' (cfr. art. 122, comma 1 del Codice)".

Per tutte le ragioni finora esposte, la soluzione ThreatMetrix, nella configurazione adottata dalle Parti e oggetto della presente istruttoria, comporta il recupero (e il successivo trattamento) di dati personali -la lista delle app installate o in esecuzione- che non risultano "strettamente necessari" alla fornitura del servizio richiesto dall'utente, per cui il loro utilizzo non può essere considerato un fingerprinting strettamente necessario all'identificazione del dispositivo.

Ne consegue che l'intero set di dati raccolti e successivamente trattati, comprensivo della suddetta lista, non può essere ricondotto, nemmeno per analogia, alla categoria dei cookie tecnici.

A differenza di questi ultimi, la soluzione ThreatMetrix viene infatti utilizzata per la raccolta di dati che eccedono il mero fingerprinting e che, potenzialmente, consentono un'attività di profilazione dell'utente, analogamente a cookie di natura commerciale (cookie "di profilazione") -non essenziali- impiegati per il tracciamento delle preferenze e delle modalità di utilizzo dell'utente finale.

Alla luce di quanto sopra, la configurazione della soluzione ThreatMetrix oggetto della presente istruttoria è sicuramente assimilabile a cookie di profilazione o commerciali, piuttosto che a cookie tecnici.

La stessa Autorità, nel già citato provvedimento n. 231 del 10 giugno 2021, infatti, ha definito i cookie di natura "non tecnica" come una "categoria in senso ampio, dal momento che l'attuale disciplina di legge, […] tesa alla tutela della confidenzialità delle comunicazioni elettroniche oltre che delle informazioni di carattere personale, è inequivocamente formulata secondo lo schema di una generale proibizione di trattamento dei dati degli interessati, salvo eccezioni rigorosamente e restrittivamente codificate, insuscettibili di estensione analogica".

Nel caso di specie, tenuto conto della non riconducibilità dell'utilizzo dei dati relativi alle app installate o in esecuzione sul dispositivo a una condizione di "stretta necessità", ne discende, a fortiori, che tali informazioni non possano essere assimilate, per analogia, ai cookie tecnici e, conseguentemente, ritenute esenti dall'obbligo di acquisizione del consenso.

Occorre altresì rilevare che, nel medesimo provvedimento, il fingerprinting è qualificato come una tecnica di tracciamento di tipo "passivo" che "permette di identificare il dispositivo utilizzato dall'utente tramite la raccolta di tutte o alcune delle informazioni relative alla specifica configurazione del dispositivo stesso adottata dall'interessato".

A tal riguardo, si evidenzia come, a differenza dei cookie (considerati degli strumenti di tracciamento "attivi") mediante i quali "l'utente che non intenda essere profilato, oltre ovviamente a poter rifiutare il proprio consenso, o a ricorrere alle tutele di carattere giuridico connesse all'esercizio dei diritti di cui al Regolamento, ha anche la possibilità pratica di rimuovere direttamente i cookie, in quanto archiviati all'interno del proprio dispositivo", nel caso di fingerprinting e di altri identificatori "passivi", "l'utente non dispone di strumenti autonomamente azionabili, dovendo necessariamente far ricorso all'azione del titolare. Ciò in quanto quest'ultimo fa uso di una tecnica di lettura che non presuppone l'archiviazione di informazioni all'interno del dispositivo dell'utente, bensì la mera osservazione delle configurazioni che lo contraddistinguono rendendolo identificabile, ed il cui esito si sostanzia in un "profilo" che resta nella sola disponibilità del titolare, cui l'interessato non ha, ovviamente, alcun accesso libero e diretto e del quale potrebbe, prima ancora, non avere neppure consapevolezza".

Quanto sopra esposto rafforza ulteriormente, in ogni caso, la necessità di una preventiva acquisizione del consenso e, se del caso, contribuisce a rendere più rigorosi i limiti all'utilizzo di informazioni per le quali l'interessato non dispone di un accesso libero e diretto e del cui effettivo impiego, talvolta, non ha neppure piena consapevolezza.

Al riguardo, dall'esame della documentazione e delle informazioni acquisite nel corso dell'istruttoria, è emerso che la fruizione del servizio offerto dalle Società tramite App risultava, nei fatti, subordinata alla concessione, da parte dell'utente, dell'autorizzazione tecnica alla raccolta dei c.d. "dati di utilizzo".

Vale la pena precisare, peraltro, che seppure le autorizzazioni tecniche implementate dai sistemi operativi consentono agli utenti di condizionare l'accesso ai dati del proprio telefono a un'azione specifica, rivelandosi meccanismo utile per la protezione dei dati dell'utente, queste non sono tuttavia progettate per un'idonea raccolta del consenso dell'utente, così come previsto dal Regolamento (cfr. artt. 4, punto 11) e 7; considerando 32), come ulteriormente chiarite nelle "Linee guida 05/2020 sul consenso ai sensi del Regolamento (UE) 2016/679" e, da ultimo, nelle "Linee guida 02/2023 sull'ambito di applicazione tecnico dell'articolo 5, paragrafo 3, della direttiva ePrivacy".

Ne consegue che, nel caso in esame, il consenso dovrebbe essere richiesto indipendentemente

dal fatto che il sistema operativo presenti (o meno) all'utente la possibilità di concedere l'autorizzazione tecnica.

Al riguardo, si precisa che, ai sensi del Regolamento, il consenso è validamente espresso solo se informato, specifico e liberamente prestato. Ciò implica, rispettivamente, che il titolare debba informare preventivamente gli interessati sugli elementi essenziali del trattamento; che la richiesta di consenso rispetti il principio di granularità, distinguendo chiaramente le diverse finalità; e che la manifestazione di volontà dell'interessato avvenga in assenza di condizionamenti, pressioni o vincoli che possano comprometterne la libertà decisionale.

In conclusione, sulla base delle valutazioni complessivamente effettuate, la condotta tenuta dalle Società in relazione al trattamento dei dati personali che comporta l'accesso a informazioni già archiviate nel terminale dell'utente ha violato, nei termini suesposti, l'art. 122 del Codice.

5.1.2 Il trattamento dei dati relativi alle app in esecuzione o comunque installate sui dispositivi degli utenti (successivo alla raccolta dei dati medesimi), per finalità di monitoraggio antifrode. Violazione dell'art. 6 del Regolamento.

Il successivo trattamento per finalità di monitoraggio antifrode dei dati relativi alle app in esecuzione o comunque installate sui dispositivi degli utenti deve, invece, essere ricondotto alla disciplina dettata dal Regolamento.

Tale trattamento deve quindi essere effettuato sulla base di una delle condizioni di liceità previste dall'art. 6, par. 1 del Regolamento, condizione che – come emerso nel corso dell'istruttoria – le Società hanno individuato nell'obbligo giuridico di cui all'art. 6, par. 1, lett. c) del Regolamento.

In particolare, secondo quanto sostenuto dalle Parti, il trattamento dei dati relativi alle app in esecuzione (o comunque installate sui dispositivi degli utenti) risulterebbe necessario per erogare agli stessi i servizi richiesti, in conformità alla normativa vigente e, in particolare, alla disciplina applicabile in materia di servizi di pagamento, la quale impone di realizzare meccanismi di monitoraggio e misure tecniche volte a garantire la sicurezza delle informazioni e delle transazioni disposte tramite canali digitali.

Si tratta, nello specifico, delle previsioni contenute negli articoli 2 e 18 degli "Standard Tecnici di Regolamentazione" emanati dell'Autorità bancaria europea (EBA) e adottati con il Regolamento Delegato (UE) 2018/389 della Commissione Europea ("Norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri") ai sensi di quanto previsto dall'art. 98 della Direttiva "PSD2".

Al riguardo, si rileva che le "Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR", adottate dall'EDPB in data 8/10/2024 (allo stato, in via di definizione a seguito di conclusa consultazione pubblica), chiariscono che l'art. 6, par. 1, lett. c) del Regolamento può essere considerato una valida base giuridica per i trattamenti di dati personali effettuati per finalità di contrasto e prevenzione delle frodi, ma ciò solo ove essi siano specificamente richiesti dalla legge applicabile (cfr. punto 107).

Tale precisazione, unitamente a quanto previsto dal Cons. 45 del Regolamento (v. sopra, par. 4.2), non consente di assumere le disposizioni sopra richiamate quale idonea base giuridica del trattamento in questione.

Le stesse infatti, che nulla dicono rispetto al trattamento dei dati personali da svolgere nell'ambito delle attività di monitoraggio delle frodi, non rispondono a quei necessari requisiti di specificità richiamati nelle Guidelines 1/2024 e nel Cons. 45 citati; in particolare, mancano di precisare "le condizioni generali (…) che presiedono alla liceità del trattamento dei dati personali" (quali i principi di trasparenza, minimizzazione e limitazione della conservazione dei dati personali), né

individuano le modalità e le finalità del trattamento antifrode posto in essere nel caso di specie.

Pertanto, le disposizioni richiamate dalle Parti a sostegno della liceità dei trattamenti in questione non costituiscono, di per sé, una idonea base giuridica, ai sensi dell'art. 6, par. 1, lett. c) del Regolamento; le stesse infatti, pur introducendo in capo ai fornitori di servizi di pagamento alcuni obblighi volti ad assicurare il rispetto della normativa antifrode, non determinano come necessari gli specifici trattamenti di dati personali in concreto posti in essere dalle Società.

Né l'argomentazione secondo cui "l'adoperabilità della base giuridica di cui all'art. 6, par. 1, lett. c) del Regolamento ha quale prerequisito non già l'esistenza di una descrizione esaustiva del trattamento medesimo contenuta nella norma di riferimento, bensì la mera presenza di una connessione funzionale e teleologica del trattamento rispetto all'obbligo normativo cui il titolare del trattamento stesso è soggetto" consente di giustificare trattamenti così invasivi.

In virtù di quanto considerato, il trattamento dei dati relativi alle app in esecuzione o comunque installate sui dispositivi degli utenti per finalità di monitoraggio antifrode avrebbe potuto essere lecitamente effettuato, sulla base di una delle altre condizioni indicate dall'art. 6, par. 1 del Regolamento; si tratta, in particolare, del consenso dell'interessato (art. 6, par. 1, lett. a)), acquisito nel rispetto delle condizioni di cui all'art. 7 del Regolamento, ovvero, in alternativa, il legittimo interesse di cui art. 6, par. 1, lett. f), purché i dati trattati non afferiscano alle particolari categorie di cui all'art. 9 del Regolamento.

In merito alla possibilità di individuare il legittimo interesse quale base giuridica dei trattamenti in questione deve tuttavia tenersi conto di quanto previsto dal Cons. 47 del Regolamento (v. sopra, par. 4.2) come meglio specificato nelle già citate "Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR" (cfr. punto 100: "the processing of personal data strictly necessary for the purposes of preventing fraud may constitute a legitimate interest of the controller. This does not mean, however, that it is automatically possible to rely on Article 6(1)(f) GDPR as a legal basis to engage in any processing of personal data for the purpose of fraud prevention, as in order to lawfully rely on Article 6(1)(f) GDPR the envisaged processing needs to be based on an interest that is legitimate and fulfill both the necessity and balancing tests" punto 100, traduzione non ufficiale: "il trattamento dei dati personali strettamente necessario ai fini della prevenzione delle frodi può costituire un legittimo interesse del titolare del trattamento. Ciò non significa, tuttavia, che sia automaticamente possibile invocare l'articolo 6, paragrafo 1, lettera f), del GDPR come base giuridica per intraprendere qualsiasi trattamento di dati personali ai fini della prevenzione delle frodi, in quanto per poter legittimamente invocare l'articolo 6, paragrafo 1, lettera f), del GDPR, il trattamento previsto deve basarsi su un legittimo interesse e soddisfare i test di necessità e di bilanciamento").

Ne discende quindi che il legittimo interesse quale condizione di liceità dei trattamenti di dati personali finalizzati alla prevenzione delle frodi non può essere applicato tout court, ma deve essere strettamente necessario a tale finalità, tenuto anche conto dei principi di minimizzazione dei dati e di limitazione della conservazione di cui all'articolo 5, paragrafo 1, lett. c) ed e) del Regolamento (vedi punto 104 Guidelines citate).

Inoltre, come previsto dall'art. 6, par. 1, lett. f) e dal Cons. 47 del Regolamento, il ricorso alla base giuridica del legittimo interesse presuppone che sia stato effettuato un attento bilanciamento con gli interessi o i diritti e le libertà fondamentali dell'interessato e l'effettuazione di tale bilanciamento deve risultare da un apposito documento di analisi, c.d. LIA (Legitimate Interest Assessment, già previsto dal Parere n. 6/2014 del WP 29 sulla nozione di legittimo interesse).

Nel caso in esame, come è emerso all'esito dell'istruttoria, tale documento di analisi non è stato redatto dalle Società.

Nessun rilievo può al riguardo essere attribuito a quanto dedotto dalle Parti, in sede di memorie difensive, ove le stesse hanno dichiarato di avere elaborato una LIA generale sulle attività antifrode "già nel 2021 e, quindi, nel contesto complessivo, anche antecedentemente alle Linee guida EDPB (intervenute solo nel 2024 e peraltro in maniera ancora non definitiva)"; è, infatti, di tutta evidenza che, trattandosi di un documento risalente nel tempo, lo stesso non prende in alcuna considerazione la specificità tecnica dei trattamenti oggetto del presente procedimento.

Pertanto, in assenza di una LIA, ovvero di una valutazione imprescindibile nel giudizio comparativo circa la prevalenza del legittimo interesse del titolare sui diritti e le libertà degli interessati - che ciascun titolare è tenuto ad effettuare, conformemente al principio di accountability -, anche la condizione di cui all'art. 6, par. 1, lett. f) del Regolamento non potrebbe essere invocata a sostegno della liceità dei trattamenti in questione.

Vero è che le Società, nelle memorie difensive, hanno vieppiù sostenuto che i trattamenti posti in essere, tramite l'applicativo ThreatMetrix, troverebbero la loro base giuridica nell'adempimento di un obbligo legale, contestando quanto prefigurato dall'Autorità, nell'atto di avvio del procedimento, ai sensi dell'art. 166, comma 5 del Codice, in ordine alla eventuale applicabilità, ai trattamenti in questione, della condizione di liceità di cui all'art.6, par.1, lett. f) del Regolamento.

Ciò in quanto, secondo le Società, "i riferimenti normativi relativi al concetto di legittimo interesse circoscrivono tale definizione a finalità proprie del titolare del trattamento che non possono essere strumentalmente traslate genericamente sugli interessati. Risulta quindi confermato l'ineludibile requisito dell'alterità tra interessato e soggetto a cui fa capo il legittimo interesse perseguito" (vengono citate, in proposito, le anzidette "Guidelines 1/2024" punto 100 e il Parere 6/2014 del WP 29).

Sul punto le Parti hanno altresì osservato come sia "insostenibile l'operazione logico-giuridica di fare sovrapporre i legittimi interessi degli interessati con quelli del titolare del trattamento", ricordando come la stessa Autorità in una recente decisione (provv. 248 del 7 luglio 2022), abbia ritenuto che "[…] i riferimenti normativi relativi al concetto di legittimo interesse, circoscrivono tale definizione a finalità proprie del titolare del trattamento che non possono essere strumentalmente traslate genericamente sugli interessati […]".

In proposito, quanto dedotto dalle parti nelle memorie difensive risulta comunque superato dal fatto che, con specifico riferimento ai trattamenti effettuati per finalità antifrode, le "Guidelines 1/2024" anzi citate specificano che non solo il titolare ma anche i clienti, così come altre terze parti, possono avere un legittimo interesse a che sia garantito che le attività fraudolente siano scoraggiate e individuate, laddove si verifichino (cfr. punto 103).

Per le ragioni sopra esposte, i trattamenti dei dati riferiti alle app in esecuzione o installate sugli smartphone degli utenti per finalità antifrode sono stati pertanto effettuati dalle Società, nei termini suesposti, in violazione del principio generale di liceità di cui all'art. 6, par. 1 del Regolamento, in quanto pur essendo riconducibili all'art. 6, par. 1, lett. f) del Regolamento (e non all'art. 6, par. 1, lett. c) sono stati effettuati in assenza di un adeguato bilanciamento con gli interessi e i diritti degli interessati.

5.2 Violazione degli artt. 5, par. 1, lett. a) e 13 del Regolamento.

Nel corso del procedimento dinanzi al Garante, sono state valutate le informative fornite agli interessati relative ai trattamenti di dati personali effettuati mediante le applicazioni mobili (App) Bancoposta e PostePay.

Nelle stesse, è specificato che "i dati personali che Poste Italiane S.p.A. tratta […] possono essere ottenuti attraverso altri canali quali, ad esempio: siti web, social network, chat, App (quali ad

esempio i dati raccolti dalla rubrica dei contatti del dispositivo per i servizi di ricarica telefonica e P2P, il numero di telefono per la trasmissione ai sistemi anti frode di Poste Italiane per proteggere i tuoi pagamenti) […]".

Da quanto anzi riportato risulta quindi che, sebbene sia stata effettivamente fornita agli interessati l'informazione relativa all'utilizzo del numero di telefono "per la trasmissione ai sistemi antifrode di Poste", nessuna informazione specifica e di dettaglio (contenente gli elementi di cui agli artt.13 e 14 del Regolamento) ha invece riguardato il complesso dei trattamenti di dati personali effettuati tramite l'applicativo ThreatMetrix.

Infatti, né da questa indicazione, né in altri passaggi dell'informativa relativa ai trattamenti di dati personali effettuati mediante le App, risulta esplicitato che le Società raccolgono in particolare, i dati riferiti alle app installate o in esecuzione nei dispositivi mobili degli utenti, allo scopo di rilevare, nell'ambito dell'attività di monitoraggio antifrode, l'eventuale presenza di programmi informatici dannosi (malware); né, a fortiori, risultano indicati gli elementi previsti dall'art. 13, par.1 e 2 del Regolamento.

In questo senso, non possono essere accolte le argomentazioni difensive delle Società secondo cui agli interessati sarebbero state rese le informazioni relative alle nuove funzionalità di sicurezza delle App attraverso l'invio, agli stessi, di un messaggio volto ad ottenere l'autorizzazione tecnica al recupero dei c.d. "dati di utilizzo" (v. par. 3.1). Ciò in quanto le informazioni rese attraverso il suddetto messaggio non soddisfano i requisiti di cui all'art. 13 del Regolamento.

Occorre infatti tenere presente che, secondo la disciplina posta dal Regolamento, un trattamento di dati personali è illecito, se l'interessato non può ragionevolmente prevederlo, sulla base del contesto e delle informazioni ricevute.

La condotta delle Società, nei termini suesposti, risulta pertanto posta in essere in violazione del principio generale di correttezza e trasparenza di cui all'art. 5, par. 1, lett. a) e dell'art. 13 del Regolamento.

Al riguardo, deve tuttavia prendersi atto che le Società, nel corso del procedimento, hanno comunicato all'Autorità di avere provveduto alla revisione delle informative sui trattamenti dei dati connessi all'uso delle app, tenendo conto dei rilievi dalla stessa formulati (documento fornito in allegato alle memorie difensive, all. sub 3).

5.3 Violazione dell'art. 28 del Regolamento.

Nel corso del procedimento sono emerse alcune criticità rispetto alla designazione del responsabile del trattamento.

Considerato infatti che a norma dell'art. 28 del Regolamento il titolare del trattamento è tenuto a ricorrere "unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate" (art. 28, par. 1, Regolamento), nel caso de quo le Società, nel designare XX quale responsabile del trattamento, hanno omesso di verificare le caratteristiche della soluzione tecnologica integrata nell'ambito della piattaforma antifrode e, quindi, in sostanza, la stessa adeguatezza delle misure tecniche e organizzative adottate dal responsabile che già si avvaleva di tale soluzione.

Infatti, dagli elementi acquisiti, è emerso che XX, nell'ambito dei diversi servizi offerti alle Società, si avvale dell'applicativo ThreatMetrix, fornito da XX, in virtù di un contratto, già in essere e precedente alla sua nomina come responsabile del trattamento, al quale, per altro verso, già nel luglio 2022 (vale a dire circa due anni prima della designazione di XX quale responsabile del trattamento) era stato affiancato un "Data Processing Addendum", che regolava, in termini generali, i trattamenti di dati personali condotti da XX per conto dei propri clienti (tra cui XX).

Sebbene le Parti fossero dunque a conoscenza dell'utilizzo, da parte di XX, di questo applicativo (il quale rappresenta per giunta una componente rilevante della piattaforma antifrode di Poste Italiane) non risulta che le stesse abbiano effettuato alcuna verifica, rispetto alle "garanzie" offerte da XX per mettere in atto "misure tecniche e organizzative adeguate".

Verifica che, ai sensi del dettato normativo dell'art. 28, par. 1 del Regolamento, risulta necessaria ai fini della corretta designazione del responsabile e per la quale non può ritenersi sufficiente – come hanno argomentato le Parti nelle memorie difensive – "l'avere ottenuto solide garanzie documentali di conformità dei responsabili del trattamento coinvolti rispetto ai requisiti di cui al Regolamento già prima dell'avvio del trattamento medesimo" (v. par. 3.1).

Inoltre, nello stesso contratto di nomina di XX quale responsabile del trattamento - sottoscritto il 04/04/2024 - non viene fatta alcuna menzione, nell'ambito dei diversi servizi offerti da XX, dei peculiari trattamenti effettuati attraverso l'applicativo ThreatMetrix.

Ciò, in violazione di quanto prescrive l'art. 28, par. 3 del Regolamento, secondo cui "I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico […] che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento […]".

Inoltre, stando a quanto stabilito dalla clausola 7.7, lett. a) del contratto tra le Società e XX, ove quest'ultima avesse voluto ricorrere ad eventuali sub-responsabili per lo svolgimento di alcune attività, la stessa avrebbe dovuto individuarli a partire dai soggetti risultanti in un elenco concordato con le Società, allegato al contratto medesimo.

Al riguardo però, nell'allegato IV al contratto - rubricato "elenco dei sub-responsabili del trattamento" -, non si rinviene alcun elenco, bensì solo l'indicazione di un nominativo, corredato da qualifica, dati di contatto e da non meglio precisate indicazioni ("Nome: XX; Nome, qualifica e dati di contatto del referente: XX – e-mail: XX", "Descrizione del trattamento (compresa una chiara delimitazione delle responsabilità qualora siano autorizzati più sub-responsabili del trattamento): Data Protection Officer").

Da tale documento non risulta, quindi, che le Società abbiano concordato con XX, alcun elenco di sub-responsabili né, nello stesso, viene menzionata espressamente XX (salvo il riferimento al dominio di posta elettronica della società nell'indirizzo XX).

Tali disallineamenti non possono essere qualificati –come hanno fatto le Società nelle argomentazioni difensive– come meri "errori materiali senza conseguenze concrete sui diritti e sulle libertà degli Interessati" dovuti ad una "erronea compilazione di alcuni moduli componenti il format standard di accordo per il trattamento dei dati di cui al menzionato art. 28 del Regolamento".

La corretta qualificazione e regolamentazione dei ruoli nel trattamento dei dati personali non è un mero adempimento formale: è una condizione strutturale per garantire liceità, trasparenza e accountability comportando chiarezza delle responsabilità giuridiche (evitando sovrapposizioni e zone grigie), corretta definizione degli obblighi di sicurezza del trattamento e pieno controllo, da parte del titolare, della catena dei subfornitori dei servizi.

La condotta sopra evidenziata risulta pertanto posta in essere in violazione dell'art. 28, par. 1 e 3 del Regolamento.

5.4 Violazione dell'art. 35 (Valutazione di impatto sulla protezione dei dati personali) e dell'art. 25 del Regolamento (privacy by design e by default)

In relazione alla violazione del principio del “privacy by design e by default” di cui all’art. 25 del Regolamento, le Società hanno rivendicato l’autonomia conferita dal Regolamento (principio di responsabilizzazione) nella scelta della soluzione tecnica più idonea all’obiettivo dichiarato di contrasto alle frodi bancarie, ritenendo “particolarmente virtuoso ed efficiente” il sistema applicativo predisposto “in ragione dell’attuale tendenza sempre crescente di frodi che caratterizzano il mercato bancario, finanziario e dei servizi di pagamento” (v. sopra par. 3.1).

Sul punto, però, le Parti si limitano a dichiarare una generica rispondenza delle misure di pseudonimizzazione e minimizzazione adottate alla normativa ed alla giurisprudenza europea (v. sopra par. 3.1), senza fornire elementi sufficientemente specifici in grado di superare le puntuali contestazioni mosse dall’Autorità circa l’insufficienza delle misure complessivamente poste in essere alla luce dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita.

Nello specifico, va precisato che la natura personale di un dato non dipende dalla presenza al suo interno di elementi identificativi diretti (quali nome, cognome, data di nascita) né dalla sua immediata intellegibilità. Anche la presenza di un singolo attributo, distinto dagli identificativi diretti ma univocamente riferibile a un individuo — ad esempio perché non condiviso con altri soggetti all’interno di un gruppo — è sufficiente a distinguere la persona a cui tale elemento si riferisce. Ciò è già di per sé idoneo a qualificare l’informazione come dato personale.

Il trattamento delle informazioni relative alle app installate e in esecuzione sul dispositivo dell’utente, in associazione peraltro con diversi identificatori univoci come indirizzi IP, ID pubblicitari, account personali o altri dati che consentono di effettuare il “fingerprinting” del dispositivo, rendono tali dati inequivocabilmente riconducibili a un individuo specifico.

Per tali motivi, quindi, le informazioni relative all’elenco delle app installate e/o in esecuzione, su un determinato dispositivo, rientrano sicuramente nella definizione di dato personale delineata nel già citato Parere 4/2007 e, di conseguenza, il loro trattamento dovrebbe conformarsi alle disposizioni in materia di protezione dei dati personali.

Inoltre, la non intellegibilità di alcune componenti del dato — o del dato nel suo complesso — non ne annulla la capacità identificativa. Possono infatti esistere dati personali intenzionalmente codificati per garantirne la confidenzialità e risultare, quindi, non immediatamente leggibili; ciò nonostante, essi conservano quella univocità che consente di riferirli a un determinato individuo e che è sufficiente a qualificarli come dati personali.

Un dato è dunque anonimo solo se è rimossa, in modo irreversibile, questa univocità, ovvero se esso può essere attribuito a più soggetti di un gruppo, o se esso non è riferito ad alcun appartenente al gruppo.

Nel caso in esame, il dato (costituito dall’elenco delle app installate – o in esecuzione - sul dispositivo dell’utente), dopo essere stato raccolto, è conservato nel sistema informatico del sub-responsabile del trattamento, previa adozione di procedure crittografiche, quali l’uso di funzioni di hash e algoritmi di cifratura, al fine di renderlo inintelligibile a terzi, ossia a soggetti diversi da quelli autorizzati.

Alla luce di tali considerazioni, l’informazione caricata nel sistema informatico del sub-responsabile, anche se inintelligibile a terzi, mantiene però interamente la propria natura di dato personale, in quanto resta univocamente associata al dato personale da cui è stata derivata, a prescindere dalla complessità della procedura utilizzata per derivarla.

Infatti, sebbene un procedimento crittografico certamente renda più difficoltosi eventuali tentativi illeciti di terzi non autorizzati di risalire ai dati originari, esso tuttavia non rimuove il collegamento

esistente tra l'informazione memorizzata nel sistema informatico e la persona a cui essa si riferisce.

Sul profilo della qualificazione giuridica della procedura crittografica che porta a ricavare dal dato originale (il pacchetto di installazione o APK, ovvero la denominazione "in chiaro" dell'app installata o in esecuzione sul dispositivo) l'informazione memorizzata nei sistemi informatici del sub-responsabile, sotto forma di stringa di testo, risulta calzante la definizione di pseudonimizzazione: il ruolo dello pseudonimo è svolto dalla stringa hash (eventualmente cifrata), memorizzata nel sistema informatico del sub-responsabile e l'informazione addizionale è costituita dal procedimento crittografico (hashing ed eventualmente l'algoritmo di cifratura applicato e la relativa chiave utilizzata), applicato dal sub-responsabile, tramite cui è ricavata, dai dati originari, la stessa stringa hash.

Peraltro, si evidenzia come il processo di recupero (lookup) del nome "in chiaro" di una app a partire dal suo pseudonimo (hash) risulti di facile e veloce esecuzione, senza particolari sforzi tecnico-computazionali, anche mediante diversi servizi disponibili in Rete (XX, XX e altri che consentono di risalire al nome del pacchetto (APK, relativo a una determinata app partendo dalla sua impronta digitale hash).

Inoltre, sempre con riferimento al sopracitato principio di protezione dei dati fin dalla progettazione e per impostazione predefinita (privacy by design e by default), che impone al titolare di limitare il trattamento alle sole informazioni strettamente necessarie, rispetto alle finalità perseguite, si rileva che non risulta effettuata dalle due Società alcuna valutazione in ordine alla effettiva necessità dei dati trattati, né emergono evidenze circa l'esame di soluzioni alternative e meno invasive.

In particolare, non risulta che siano state considerate misure tecniche o organizzative diverse, idonee a perseguire le medesime finalità, quali, ad esempio, l'adozione di ulteriori meccanismi di protezione alternativi all'utilizzo delle informazioni relative alle app installate e/o in esecuzione (cfr. par. 5.1.1), ovvero la limitazione del trattamento alla sola verifica della presenza di app ritenute a rischio per la sicurezza, con conseguente esclusione o minimizzazione del trattamento dei dati riferiti alle app non qualificate come malevole.

Anche con riguardo alla mancata effettuazione della valutazione d'impatto ai sensi dell'art. 35 del Regolamento, le osservazioni addotte dalle Società nel procedimento pertengono ad aspetti secondari e non al merito della contestazione; ciò in quanto si concentrano sulla critica di un supposto automatismo tra violazione dell'art. 35 e violazione dell'art. 25 del Regolamento (mai sostenuto dall'Autorità) nonché sul fatto di aver comunque svolto valutazioni di impatto, valutazioni che tuttavia non sono risultate adeguate ai fini del rispetto di cui all'obbligo dell'art. 35 del Regolamento, in quanto indubbiamente non riferite alle specifiche tecnologie oggetto del presente procedimento.

Infatti le Società hanno affermato, peraltro solo in sede ispettiva, di non aver proceduto a una specifica valutazione di impatto, riferita ai trattamenti in questione, in quanto essa sarebbe stata effettuata, in via generale e complessiva, nel "Data Protection Impact Assessment – Prevenzione Frodi attraverso la Piattaforma Integrata Anti Frode (PIAF)" con riferimento a tutti i trattamenti dei dati personali necessari allo svolgimento delle attività antifrode.

Tuttavia, dall'analisi del citato documento (fornito dai contitolari), sono emerse diverse incongruenze con riferimento ai dati personali oggetto del trattamento in esame.

In particolare, è stato verificato che tale documento riporta solo i seguenti tipi di dati oggetto del trattamento:

Dati identificativi: CF, coordinate bancarie (IBAN), IP, numero libretto postale o numero

carta, partita IVA, dati di contatto, indirizzo e-mail o pec, numero di telefono fisso o mobile, indirizzo di domicilio o di recapito;

Dati anagrafici: cognome, nome, indirizzo di residenza;

Dati relativi alla posizione economica e finanziaria: transazioni finanziarie (pagamenti o incassi);

Dati di geolocalizzazione.

Come risulta evidente da tale descrizione, tra i tipi di dati elencati non figurano affatto i dati relativi alle app installate o in esecuzione sul dispositivo dell'utente, i dati che consentono di effettuare il "fingerprinting" del dispositivo e i diversi altri identificativi utilizzati dalla soluzione oggetto del presente procedimento.

Occorre considerare che la finalità del documento di valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment - DPIA) è proprio quella di individuare (e mitigare) i rischi derivanti dal trattamento di dati personali, soprattutto nei casi in cui tale trattamento possa comportare un rischio elevato per i diritti e le libertà degli interessati, come previsto dall'art. 35 del Regolamento.

Si tratta quindi di uno degli elementi di maggiore rilevanza previsti dalla normativa in materia di protezione dati, in quanto esprime pienamente la responsabilizzazione (accountability) dei titolari nei confronti dei trattamenti di dati personali da questi effettuati.

A tal proposito, le Linee-guida del Gruppo Articolo 29, in materia di valutazione di impatto sulla protezione dei dati (WP248, adottate il 4 ottobre 2017), offrono alcuni chiarimenti sul tema e precisano come la DPIA debba essere necessariamente interpretata come un processo soggetto a revisione continua, piuttosto che un adempimento una tantum.

Gli stessi contitolari, nel corso dell'attività ispettiva svolta, hanno confermato quanto inizialmente dichiarato ovvero che "le misure di tutela degli Interessati implementate (in particolare, la codifica delle informazioni in formato hash MD5 e l'assenza di trattamento in chiaro d'informazioni inerenti al nome delle applicazioni rilevate, a elementi multimediali o altre informazioni riservate dell'Interessato), hanno condotto a escludere la presenza di un rischio elevato per i diritti e le libertà delle persone fisiche e conseguentemente la necessità di svolgere una valutazione d'impatto sulla protezione dei dati a norma dell'art. 35 del RGPD".

Tali incongruenze evidenziano tuttavia un approccio complessivamente non in linea con i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita (privacy by design e by default) di cui all'art. 25, parr. 1 e 2, del Regolamento, che richiedono che il trattamento sia configurato prevedendo, fin dall'inizio, le garanzie indispensabili "al fine di soddisfare i requisiti" del Regolamento a tutela dei diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

In fase progettuale, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", i titolari avrebbero dovuto infatti effettuare un'analisi preventiva di cui rendere conto all'Autorità, in sede istruttoria. Una di tali attività sarebbe stata proprio l'effettuazione di un'attenta valutazione di impatto per garantire la conformità delle scelte effettuate ai suddetti principi di protezione dei dati personali.

Su questa linea interpretativa, anche la Suprema Corte di Cassazione ha affermato che "il sistema di tutela dei dati personali deve porre l'utente al centro, così obbligando il titolare del trattamento ad una tutela effettiva da un punto sostanziale, non solo formale: non è sufficiente, cioè, che la progettazione del sistema sia conforme alla norma se, poi, l'utente non è tutelato. Dall'art. 25

suddetto si evince, allora, che l'approccio del menzionato Regolamento UE è centrato, tra l'altro, sulla valutazione del rischio (risk based approach), per cui le aziende devono valutare il rischio inerente alle loro attività. Con tale valutazione si determina la misura di responsabilità del titolare o del responsabile del trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti. Tale valutazione del rischio va fatta al momento della progettazione del sistema, quindi prima che il trattamento inizi" (Cassazione civile, sez. I, 11/10/2023).

La conferma indiretta della pertinenza delle argomentazioni sopra svolte appare infine confermata dalla circostanza che le Società hanno ritenuto, procedimento durante, di avviare la redazione della DPIA, dichiarando nelle memorie difensive che il documento è in corso di predisposizione.

La condotta sopra evidenziata risulta pertanto posta in essere in violazione degli artt. 25 e 35 del Regolamento.

5.5 Violazione dell'art. 32 del Regolamento.

[OMISSIS]

5.6 Violazione dell'art. 5, par. 1, lett. e) del Regolamento.

Con riguardo ai tempi di conservazione dei dati raccolti e memorizzati nei sistemi ThreatMetrix di XX, le Società negano la violazione dell'art. 5, par. 1, lett. e) del Regolamento, dichiarando che "il presunto disallineamento tra il periodo di conservazione dei Dati inizialmente dichiarato a codesta onorevole Autorità e quello effettivo è di entità minima, pari solo a quattro mesi e comunque corrisponde al tempo tecnico necessario ad assicurare la cancellazione sicura dei Dati in esame. Più nel dettaglio, sulla base delle informazioni messe a disposizione dal fornitore di ThreatMetrix, i Dati sottoposti a cifratura tramite hashing sono conservati nella base dati analitica per un massimo di ventotto mesi, anziché ventiquattro, per garantire un'adeguata rappresentazione dei fenomeni".

Al riguardo, quanto sopra affermato dalle Parti sul "tempo tecnico necessario ad assicurare la cancellazione sicura dei dati", non può ritenersi idoneo a giustificare la protrazione del periodo di conservazione di quattro mesi rispetto a quanto inizialmente dichiarato.

Tale affermazione, intanto, è in contrasto con quanto descritto dai documenti tecnici del sub-responsabile, laddove emerge che "i dati sono utilizzati dagli analisti di ThreatMetrix per il miglioramento delle analisi e lo sviluppo di nuove funzionalità" ("the data is used by ThreatMetrix data analysts for improvements of analytics and creation of new features") e non, pertanto, per eseguire presunte operazioni tecniche di cancellazione che si protraggono oltre i tre mesi.

Inoltre, tale operazione risulterebbe, da un punto di vista tecnico, comunque di difficile comprensione e giustificazione. Sempre a tal proposito, le Parti hanno difatti rappresentato a questa Autorità che "La cancellazione dei dati con una storicità superiore a 28 mesi presenti nel database di Analytics è effettuata sul cluster framework XX tramite una procedura gestita da un processo automatizzato giornaliero" (riscontro informativo del 25 novembre 2024); da ciò si evince, quindi, che: la procedura di cancellazione è eseguita dopo 28 mesi (che quindi è individuato come tempo effettivo di conservazione) e che tale procedura ha dei tempi di esecuzione ordinari, in quanto "gestita da un processo automatizzato giornaliero".

Inoltre, l'affermazione delle Parti per la quale "i Dati […] sono conservati nella base dati analitica per un massimo di ventotto mesi, anziché ventiquattro, per garantire un'adeguata rappresentazione dei fenomeni" è troppo vaga e indeterminata, in quanto non individua una precisa finalità, né un criterio oggettivo di necessità che giustifichi tale periodo aggiuntivo, ma solamente un'esigenza "statistica" non meglio precisata.

Il principio di limitazione della conservazione richiede che il periodo di conservazione sia proporzionato alla una finalità del trattamento determinata, esplicita e legittima.

Di conseguenza, si evidenzia come, nel corso del procedimento, non sia stata fornita una motivazione idonea all'ulteriore periodo di tempo, eccedente di quattro mesi i tempi di conservazione dei dati gestititi attraverso il sistema PIAF (Piattaforma Integrata Anti Frode), piattaforma inserita nell'infrastruttura informatica di Poste Italiane che, pur partecipando ai medesimi trattamenti dei sistemi ThreatMetrix, conserva i dati per un periodo massimo di 24 mesi.

Ne consegue che il periodo eccedente, rispetto ai ventiquattro mesi inizialmente dichiarati, non può essere qualificato come fase meramente strumentale alla cancellazione, ma costituisce, a tutti gli effetti, un'ulteriore conservazione funzionale al trattamento, in contrasto con il suddetto principio di limitazione della conservazione.

L'eventuale esigenza di disporre di un arco temporale più ampio per finalità statistiche, infatti, avrebbe dovuto essere valutata e formalizzata ex ante, mediante una coerente definizione del periodo di conservazione e la sua comunicazione agli interessati.

Tali elementi hanno comportato pertanto la violazione del principio di limitazione della conservazione di cui all'art. 5, par.1, lett. e) del Regolamento.

6. Conclusioni: dichiarazione di illiceità del trattamento.

Alla luce di quanto complessivamente rilevato, l'Autorità ritiene che le dichiarazioni, la documentazione e le ricostruzioni fornite dai titolari del trattamento nel corso dell'istruttoria, non consentano di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e che risultino pertanto inidonee a disporre l'archiviazione del presente procedimento, non ricorrendo peraltro alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Il trattamento dei dati personali dei clienti effettuato per il tramite delle app Bancoposta e PostePay, risulta infatti illecito, nei termini su esposti, in quanto posto in essere in violazione degli artt. 5, 6, 13, 25, 28, 32, 35 del Regolamento, nonché con l'art. 122 del Codice in materia di protezione dei dati personali.

La violazione delle disposizioni sopra richiamate comporta l'applicazione della sanzione amministrativa prevista dall'art. 83, par. 4, lett. a) e par. 5, lett. a) e b) del Regolamento, visto anche l'art. 166, c. 2 del Codice.

7. Misure correttive (art. 58, par. 2, lett. d) ed f), del Regolamento).

L'art. 58, par. 2, del Regolamento attribuisce al Garante il potere di "ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine" (lett. d), nonché di "imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento" (lett. f).

In tale quadro, tenuto conto che i trattamenti esaminati sono risultati illeciti in quanto privi di una valida base giuridica ai sensi dell'art. 6 del Regolamento (v. par. 5.1.), si ingiunge alle Società, ai sensi dell'art. 58, par. 2, lett. f), del Regolamento, di interrompere i trattamenti svolti mediante l'applicativo ThreatMetrix e consistenti nella raccolta dei dati del dispositivo relativi all'utilizzo delle app installate e/o in esecuzione, come descritti nell'ambito del presente provvedimento.

Inoltre, tenuto conto che la procedura di cancellazione dei dati raccolti è da considerarsi, allo stato, eseguita dopo 28 mesi e, pertanto, in violazione del principio di limitazione della conservazione (v. supra, par. 5.6.), si ritiene altresì necessario ingiungere alle Società, ai sensi

dell'art. 58, par. 2, lett. d) del Regolamento, qualora le stesse non abbiano già provveduto, di individuare specifiche tempistiche di conservazione dei dati degli utenti i cui dati sono trattati mediante l'applicativo ThreatMetrix; ciò in linea con il principio di limitazione della conservazione sancito dall'art. 5, par. 1, lett. e) del Regolamento.

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

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

Il Garante, ai sensi dell'art. 58, par. 2, lett. i) del Regolamento e dell'art. 166 del Codice, ha il potere di infliggere una sanzione amministrativa pecuniaria prevista dall'art. 83 del Regolamento, mediante l'adozione di una ordinanza ingiunzione (art. 18. L. 24 novembre 1981 n. 689), in relazione al trattamento dei dati personali posto in essere da Poste Italiane S.p.A. e PostePay S.p.A., di cui è stata accertata l'illiceità, nei termini sopra esposti.

Ritenuto di dover applicare il paragrafo 3 dell'art. 83 del Regolamento laddove prevede che "se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento […] viola, con dolo o colpa, varie disposizioni del presente Regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave", l'importo totale della sanzione è calcolato in modo da non superare il massimo edittale previsto dal medesimo art. 83, par. 5 del Regolamento.

L'Autorità, alla luce delle Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del Regolamento adottate il24 maggio 2023, alle quali sono state apportate lievi modifiche il 29 giugno 2023, ha dunque tenuto conto del livello elevato di gravità delle violazioni, sulla base di tutti i fattori rilevanti nel caso concreto, e in particolare la natura, della gravità e della durata delle violazioni, tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito.

L'Autorità ha altresì preso in considerazione i criteri relativi al carattere doloso o colposo delle violazioni e le categorie di dati personali interessate dalle violazioni, nonché la maniera in cui l'autorità di controllo ha preso conoscenza della violazione (v. art. 83, par. 2 e Considerando 148 del Regolamento).

Infine, tenuto conto che Poste Italiane e Postepay sono contitolari del trattamento e che, pertanto, la responsabilità per le violazioni del Regolamento sussiste in capo a ciascuna Società (cfr. art. 5 l. 689/81 "Quando più persone concorrono in una violazione amministrativa, ciascuna di esse soggiace alla sanzione per questa disposta, salvo che sia diversamente stabilito dalla legge"), si provvede a disporre l'ordinanza ingiunzione separatamente per ciascuna società, come di seguito.

8.1 Ordinanza di ingiunzione nei confronti di Poste Italiane S.p.a.

Con riferimento agli elementi elencati dall'art. 83, par. 2, del Regolamento ai fini dell'applicazione della sanzione amministrativa pecuniaria e la relativa quantificazione nei confronti di Poste Italiane S.p.a. tenuto conto che la sanzione deve "in ogni caso [essere] effettiva, proporzionata e dissuasiva" (art. 83, par. 1 del Regolamento), si rappresenta che, nel caso di specie, sono state tenute in considerazione le circostanze sotto riportate:

- in relazione alla natura, gravità e durata delle violazioni, è stata considerata rilevante la natura delle stesse e alto il livello di gravità in quanto concernenti l'inosservanza dei principi

generali del trattamento e, in particolare, il principio di liceità e di trasparenza, di limitazione della conservazione nonché il generale principio di “accountability”. Altresì, si è tenuto conto della particolare invasività dei trattamenti posti in essere, che hanno comportato l’accesso a dati registrati sul dispositivo, potenzialmente anche in grado di rivelare informazioni a carattere particolare o, comunque, oggetto di una specifica tutela da parte del Regolamento.

- con riferimento al carattere doloso o colposo della violazione e al grado di responsabilità, è stato preso in considerazione il comportamento significativamente negligente e il rilevante grado di responsabilità in ordine alla erronea individuazione della base giuridica dei trattamenti effettuati, alla mancata predisposizione di idonee misure di sicurezza e all’obbligo di svolgere la preventiva valutazione di impatto dei trattamenti posti in essere. È stata inoltre considerata la mancata verifica delle caratteristiche della soluzione tecnologica offerta dal Responsabile del trattamento e, quindi, la adeguatezza delle misure adottate dal medesimo;

- l’elevato numero di soggetti coinvolti dalle violazioni, identificabile in alcuni milioni di utenti interessati;

- in relazione alle misure adottate dal contitolare del trattamento per attenuare il danno subito dagli interessati, fermo restando che l’illiceità dei trattamenti riguarda il tracciamento sia delle app installate che di quelle in esecuzione, si è tenuto conto di quanto dichiarato dalle parti nel corso del procedimento in ordine all’avvenuta rimozione dell’obbligo -per gli utenti- di fornire il consenso per il recupero delle informazioni relative alle app in esecuzione sui dispositivi e che “agli [stessi] è stata offerta la possibilità di revocare l’eventuale consenso precedentemente reso […] (v. par 3.2);

- a favore della parte, il grado di cooperazione con l’Autorità e l’impegno dimostrato dalla stessa che, nel corso del procedimento, ha provveduto a revisionare una serie di documenti, al fine di adeguarli alla normativa richiamata dall’Autorità (informativa sul trattamento dei dati personali ai sensi dell’art. 13 del Regolamento, contratto per il trattamento dei dati personali ex art. 28 del Regolamento);

- a favore della parte, si è tenuto altresì conto del fatto che non risultino precedenti violazioni commesse o precedenti provvedimenti di cui all’art. 58 del Regolamento relativamente allo stesso oggetto.

Si ritiene, inoltre, che assumano rilevanza, nell’ipotesi di specie, in ragione dei richiamati principi di effettività, proporzionalità e dissuasività ai quali l’Autorità deve attenersi nella determinazione dell’ammontare della sanzione (art. 83, par. 1, del Regolamento), le condizioni economiche del contravventore, determinate in base al volume d’affari di Poste Italiane S.p.a., di cui al bilancio d’esercizio per l’anno 2024 (ultimo disponibile).

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di applicare nei confronti di Poste Italiane S.p.a. la sanzione amministrativa del pagamento di una somma pari ad euro 6.624.000,00 (sei milioni seicentoventiquattromila/00).

8.2 Ordinanza di ingiunzione nei confronti di Postepay S.p.a.

Con riferimento agli elementi elencati dall’art. 83, par. 2, del Regolamento ai fini dell’applicazione della sanzione amministrativa pecuniaria e la relativa quantificazione nei confronti di Postepay S.p.a. tenuto conto che la sanzione deve “in ogni caso [essere] effettiva, proporzionata e dissuasiva” (art. 83, par. 1 del Regolamento), si rappresenta che, nel caso di specie, sono state tenute in considerazione le circostanze sotto riportate:

- in relazione alla natura, gravità e durata delle violazioni, è stata considerata rilevante la natura delle stesse in quanto concernenti l’inosservanza dei principi generali del trattamento

e, in particolare, il principio di liceità e di trasparenza, di limitazione della conservazione nonché il generale principio di “accountability”. Altresì, si è tenuto conto della particolare invasività dei trattamenti posti in essere, che hanno comportato l’accesso a dati registrati sul dispositivo, potenzialmente anche in grado di rivelare informazioni a carattere particolare o, comunque, oggetto di una specifica tutela da parte del Regolamento;

- con riferimento al carattere doloso o colposo della violazione e al grado di responsabilità del contitolare Postepay S.p.a., è stato preso in considerazione il comportamento significativamente negligente e il rilevante grado di responsabilità del contitolare in ordine alla mancata predisposizione di idonee misure di sicurezza e all’obbligo di svolgere la preventiva valutazione di impatto dei trattamenti posti in essere. È stata inoltre considerata la mancata verifica delle caratteristiche della soluzione tecnologica offerta dal Responsabile del trattamento e, quindi, la adeguatezza delle misure adottate dal medesimo;

- l’elevato numero di soggetti coinvolti dalle violazioni, identificabile in alcuni milioni di utenti interessati;

- in relazione alle misure adottate dal contitolare del trattamento per attenuare il danno subito dagli interessati, fermo restando che l’illiceità dei trattamenti riguarda il tracciamento sia delle app installate che di quelle in esecuzione, si è tenuto conto di quanto dichiarato dalle parti nel corso del procedimento in ordine all’avvenuta rimozione dell’obbligo -per gli utenti- di fornire il consenso per il recupero delle informazioni relative alle app in esecuzione sui dispositivi e che “agli [stessi] è stata offerta la possibilità di revocare l’eventuale consenso precedentemente reso […] (v. par 3.2);

- a favore della parte, il grado di cooperazione con l’Autorità e l’impegno dimostrato dalla stessa che, nel corso del procedimento, ha provveduto a revisionare una serie di documenti al fine di adeguarli alla normativa richiamata dall’Autorità (informativa sul trattamento dei dati personali ai sensi dell’art. 13 del Regolamento, contratto per il trattamento dei dati personali ex art. 28 del Regolamento);

- a favore della parte, si è tenuto altresì conto del fatto che non risultino precedenti violazioni commesse o precedenti provvedimenti di cui all’art. 58 del Regolamento relativamente allo stesso oggetto.

Si ritiene, inoltre, che assumano rilevanza, nell’ipotesi di specie, in ragione dei richiamati principi di effettività, proporzionalità e dissuasività ai quali l’Autorità deve attenersi nella determinazione dell’ammontare della sanzione (art. 83, par. 1, del Regolamento), le condizioni economiche del contravventore, determinate in base al volume d’affari di Postepay S.p.a. di cui al bilancio d’esercizio per l’anno 2024 (ultimo disponibile).

Alla luce degli elementi sopra indicati e delle valutazioni effettuate si ritiene, nel caso di specie, di applicare nei confronti di Postepay S.p.a. la sanzione amministrativa del pagamento di una somma pari ad euro 5.877.000,00 (cinque milioni ottocentosettantasettemila/00).

9. Pubblicazione del capo contenente l’ordinanza ingiunzione sul sito Internet del Garante.

In tale quadro, considerato si ritiene che, ai sensi dell’art. 166, comma 7, del Codice e dell’art. 16, comma 1, del Regolamento del Garante n. 1/2019, considerato l'alto livello di gravità delle violazioni e l'elevato numero di interessati coinvolti, si debba procedere alla pubblicazione del capo 8 del presente provvedimento, contenente l’ordinanza ingiunzione nei confronti delle due Società, sul sito Internet del Garante.

Ciò anche in considerazione della tipologia delle violazioni accertate che hanno riguardato i principi generali, tra cui in particolare le condizioni di liceità del trattamento e l’assenza di una

adeguata informativa agli utenti.

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi degli artt. 57, par. 1, lett. f) e 83, del Regolamento, rileva l'illiceità del trattamento effettuato da Poste Italiane S.p.a., , con sede legale in Roma, Viale Europa 190, C.F. n. 01114601006 e da Postepay S.p.a., con sede legale in Roma, Viale Europa 190, C.F. n. 06874351007, in qualità di contitolari del trattamento, nei termini di cui in motivazione, per la violazione degli artt. 5, 6, 13, 25, 28, 32, 35 del Regolamento, nonché dell'art. 122 del Codice in materia di protezione dei dati personali;

ORDINA

a Poste Italiane S.p.a.:

- ai sensi dell'art. 58, par. 2, lett. i) del Regolamento, di pagare la somma di euro 6.624.000,00 (sei milioni seicentoventiquattromila/00), a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento;

- ai sensi dell'art. 58, par. 2, lett. d) del Regolamento di individuare specifiche tempistiche di conservazione dei dati degli utenti i cui dati sono tuttora trattati mediante l'applicativo ThreatMetrix, entro 30 giorni dalla notifica del presente provvedimento;

- ai sensi dell'art. 58, par. 2, lett. f) del Regolamento di interrompere i trattamenti relativi alla raccolta di dati del dispositivo sulle app installate e/o in esecuzione, entro 10 giorni dalla notifica del presente provvedimento.

e a Postepay S.p.a.

- ai sensi dell'art. 58, par. 2, lett. i) del Regolamento, di pagare la somma di euro 5.877.000,00 (cinque milioni ottocentosettantasettemila/00) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento;

- ai sensi dell'art. 58, par. 2, lett. d) del Regolamento di individuare specifiche tempistiche di conservazione dei dati degli utenti i cui dati sono tuttora trattati mediante l'applicativo ThreatMetrix, entro 30 giorni dalla notifica del presente provvedimento;

- ai sensi dell'art. 58, par. 2, lett. f) del Regolamento di interrompere i trattamenti relativi alla raccolta di dati del dispositivo sulle app installate e/o in esecuzione, entro 10 giorni dalla notifica del presente provvedimento.

Entro i termini sopra individuati, le Società dovranno conformarsi alle prescrizioni di cui al par. 7 del presente provvedimento e inviare all'Autorità un riscontro adeguatamente documentato ai sensi dell'art. 157 del Codice; l'eventuale mancato riscontro può comportare l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, lett. e) del Regolamento.

INGIUNGE

• a Poste Italiane S.p.a. di pagare la predetta somma di euro 6.624.000,00 (sei milioni seicentoventiquattromila/00), secondo le modalità indicate in allegato, entro 30 giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dell'art. 27 della legge n. 689/1981;

• a Postepay S.p.a. di pagare la predetta somma di euro 5.877.000,00 (cinque milioni

ottocentosettantasettemila/00), secondo le modalità indicate in allegato, entro 30 giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dell'art. 27 della legge n. 689/1981.

Si ricorda che resta salva la facoltà per il trasgressore di definire la controversia mediante il pagamento – sempre secondo le modalità indicate in allegato - di un importo pari alla metà della sanzione irrogata, entro il termine di cui all'art. 10, comma 3, del d. lgs. n. 150 dell'1.9.2011 previsto per la proposizione del ricorso come sotto indicato (art. 166, comma 8, del Codice);

DISPONE

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

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

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

Ai sensi dell'art. 78 del Regolamento, nonché degli articoli 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo individuato nel medesimo art. 10, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 17 aprile 2026

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Montuori