PRATICHE COMMERCIALI SCORRETTE

PS12768 - APP BANCO POSTA-RICHIESTA AUTORIZZAZIONI
Provvedimento n. 31566

L'AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO

NELLA SUA ADUNANZA del 20 maggio 2025;

SENTITO il Relatore, Saverio Valentino;

VISTA la Parte II, Titolo III, del Decreto Legislativo 6 settembre 2005, n. 206, e successive modificazioni (di seguito, "Codice del consumo");

VISTO il "*Regolamento sulle procedure istruttorie in materia di pubblicità ingannevole e comparativa, pratiche commerciali scorrette, violazione dei diritti dei consumatori nei contratti, violazione del divieto di discriminazioni e clausole vessatorie*" (di seguito, "Regolamento"), adottato dall'Autorità con delibera del 1° aprile 2015, n. 25411, successivamente sostituito dal "*Regolamento sulle procedure istruttorie nelle materie di tutela del consumatore e pubblicità ingannevole e comparativa*" (di seguito, "Nuovo Regolamento"), adottato dall'Autorità con delibera del 5 novembre 2024, n. 31356;

VISTA la comunicazione del 22 aprile 2024, con cui è stato avviato il procedimento PS12768 nei confronti della società Poste Italiane S.p.A.;
TENUTO CONTO degli incontri svolti con il Garante per la protezione dei dati personali nelle date 11 aprile 2024, 4 giugno 2024, 19 settembre 2024 e 14 gennaio 2025 e di quelli svolti con il medesimo Garante e con Banca d'Italia nelle date 24 settembre 2024 e 7 ottobre 2024.

VISTE le proprie decisioni del 10 settembre 2024, 15 novembre 2024, 10 gennaio 2025, 5 marzo 2025 e 15 aprile 2025 con le quali, ai sensi dell'articolo 7, comma 3, del Regolamento e dell'articolo 8, comma 4, del Nuovo Regolamento, è stata disposta la proroga del termine di conclusione del procedimento complessivamente fino al 1° luglio 2025;

VISTI gli atti del procedimento;

I. LA PARTE

1. Poste Italiane S.p.A., P.IVA 01114601006, in qualità di Professionista, ai sensi dell'articolo 18, comma 1, lettera b), del Codice del consumo (di seguito, anche "Poste Italiane", "Professionista" o "Società").
Poste Italiane offre differenti tipologie di servizi tra cui figurano quelli riguardanti la fornitura di conti correnti e carte prepagate, quali Banco Posta e PostePay, in relazione ai quali riconosce la possibilità di operare *online*, anche attraverso le relative *App*, disponendo pagamenti, ricevendo somme di denaro e compiendo le principali operazioni bancarie e finanziarie[1]. Dal bilancio di

[1] Sul sito *web* del Professionista, relativamente *all'App* Banco Posta, è riportato che "*Con App Banco Posta puoi anche:*
- ***Controllare** con semplicità il tuo saldo e tenere sempre sotto controllo e in tempo reale le tue spese;*
- ***autorizzare** velocemente con Codice PosteID tutte le tue operazioni e visualizzare il PIN del tuo conto corrente, del tuo Libretto Smart e delle tue Carte prepagate PostePay nel «Dettaglio» del tuo rapporto;*

esercizio consolidato al 31 dicembre 2023, risultano ricavi pari a 11.989 milioni di euro, con un EBITDA pari a 3.431 milioni di euro[2].

II. LA PRATICA COMMERCIALE OGGETTO DEL PROCEDIMENTO

2. Il procedimento concerne il comportamento posto in essere dal Professionista consistente nell'aver subordinato l'utilizzo delle *App* Banco Posta e PostePay - installate sugli *smartphone* con sistema operativo Android - al rilascio dell'autorizzazione da parte dell'utente ad accedere ai dati del proprio *smartphone*, pena il blocco delle medesime *App*. La condotta in esame, posta in essere da Poste Italiane a partire dall'aprile 2024, risulta contraria alla diligenza professionale e caratterizzata da profili di aggressività, in violazione degli articoli 20, 24 e 25 del Codice del consumo.

III. LE RISULTANZE DEL PROCEDIMENTO

III.1. L'iter del procedimento

3. In relazione alla condotta descritta, sulla base delle segnalazioni pervenute all'Autorità a partire dal mese di aprile 2024 e degli accertamenti preistruttori effettuati, in data 22 aprile 2024[3] è stato avviato il procedimento istruttorio PS12768 nei confronti della società Poste Italiane S.p.A. per possibile violazione degli articoli 20, 24 e 25 del Codice del consumo.

4. In particolare, in tale sede, è stata contestata la pratica commerciale scorretta consistente nel blocco dell'utilizzo delle *App* Banco Posta e PostePay - installate negli *smartphone* con sistema operativo Android - in caso di mancato rilascio, da parte degli utenti, dell'autorizzazione ad accedere ai dati del proprio *smartphone*. In considerazione delle specificità del caso di specie, avente a oggetto alcune segnalazioni da parte di consumatori che lamentavano la richiesta proveniente da Poste Italiane di accesso ai dati personali del proprio *smartphone* per potere utilizzare le *App* di Poste Italiane, in data 11 aprile 2024, gli Uffici hanno incontrato i rappresentanti del Garante per la protezione dei dati personali (di seguito anche "GPDP")[4].

- ***prelevare*** *dal tuo conto corrente, dal tuo Libretto Smart e dalle tue Carte prepagate PostePay presso tutti gli ATM Postamat senza utilizzare la carta e premendo solo il tasto 9;*
- ***pagare*** *il bollo della tua auto o della tua moto;*
- ***inviare denaro*** *da Conto corrente Banco Posta tramite bonifico e Postagiro;*
- ***apportare*** *liquidità sul tuo Libretto con un girofondo o associando l'Iban del tuo conto corrente bancario;*
- ***acquistare*** *Buoni Fruttiferi Postali e attivare l'Offerta Supersmart;*
- ***gestire e personalizzare*** *i limiti delle tue carte di debito e prepagate PostePay, definire le zone geografiche di utilizzo e le tipologie di spesa;*
- ***trovare*** *i negozi aderenti al programma ScontiPoste*"

Quanto, invece, *all'App* PostePay, sempre sul medesimo sito, si riporta: "***In sintesi Paghi*** *Paghi contactless o inquadrando con il tuo* smartphone *il* QR Code *per i bollettini e per i pagamenti nei negozi convenzionati e autorizzi tutto con PosteID.* ***Ricarichi*** *Ricarichi la tua Carta PostePay anche con conti e carte di altre banche abilitate con il Servizio PostePay Open.* ***Trasferisci*** *Fai bonifici o trasferisci denaro in Italia e, grazie al servizio Western Union, anche all'estero.* ***Gestisci carta e SIM*** *Controlli i movimenti della tua Carta PostePay, ricarichi la tua SIM PosteMobile, verifichi il credito e i* bonus *residui del tuo piano tariffario, visualizzi i dettagli del traffico.* ***Trovi punti vendita*** *Trovi i negozi aderenti a ScontiPoste, gli Uffici Postali, gli ATM più vicini e la stazione di servizio IP preferita per fare rifornimento.* ***Condividi*** *Trasferisci denaro da una PostePay ad un'altra PostePay con il P2P. Se hai attiva sulla tua SIM l'offerta PostePay Connect, con il G2G puoi condividere i tuoi giga.*".

[2] Cfr. "*Relazione Finanziaria Annuale 2023*" in https://www.posteitaliane.it/it/bilanci-e-relazioni.html#/.

[3] Doc. n. 10 (Comunicazione di avvio del procedimento - prot. n. 0041643 del 22/04/2024).

[4] Doc. n. 6 (Resoconto incontro dell'11/04/2024 con i rappresentanti del Garante per la protezione dei dati personali).

5. In data 13 maggio 2024, Poste Italiane ha presentato una memoria e dato riscontro alle informazioni richieste nella comunicazione di avvio del procedimento[5].
6. In data 4 giugno 2024, gli Uffici hanno incontrato nuovamente i rappresentanti del GPDP per proseguire il confronto e fornire a tale Autorità gli aggiornamenti sul procedimento in corso[6].
7. In data 6 giugno 2024[7], Poste Italiane ha depositato un'ulteriore memoria (successivamente integrata in data 14 giugno 2024[8]) e, contestualmente, ha presentato una proposta di impegni, ai sensi dell'articolo 27, comma 7, del Codice del consumo, volti a rimuovere i profili di scorrettezza della condotta oggetto di contestazione.
8. In data 18 giugno 2024, dando seguito a una richiesta formulata dalla Parte, Poste Italiane è stata sentita in audizione[9] e, nel corso della stessa, sono state formulate ulteriori richieste di informazioni, riscontrate dal Professionista il 18 luglio 2024[10].
9. Nell'adunanza del 10 settembre 2024, l'Autorità ha esaminato la predetta proposta di impegni e ne ha deliberato il rigetto per l'interesse all'accertamento dell'eventuale infrazione, nonché per l'inidoneità degli stessi a sanare tutti i profili di scorrettezza contestati con la comunicazione di avvio del procedimento[11].
10. In data 19 settembre 2024, gli Uffici hanno incontrato nuovamente i rappresentanti del GPDP e hanno concordato di organizzare un ulteriore incontro al fine di mantenere costante il coordinamento delle rispettive attività coinvolgendo anche i rappresentanti di Banca d'Italia, in qualità di autorità di regolazione competente[12].
11. Pertanto, in data 24 settembre 2024, si è svolto un incontro tra gli Uffici e i rappresentanti delle suddette autorità nel corso del quale si è concordato di aggiornarsi nuovamente e reciprocamente a seguito dei rispettivi approfondimenti sulla fattispecie oggetto del procedimento[13].
12. In data 26 settembre 2024, è stata formulata alla Parte un'ulteriore richiesta di informazioni[14] che è stata riscontrata dalla Società il 17 ottobre 2024[15] e integrata il 22 ottobre 2024[16].
13. In data 7 ottobre 2024, si è svolto un ulteriore incontro tra gli Uffici e i rappresentanti del GPDP e di Banca d'Italia per un reciproco confronto sulle verifiche e sugli approfondimenti effettuati,

5 Doc. n. 14 (Trasmissione documenti - prot. n. 0048105 del 13/05/2024).
6 Doc. n. 15 (Resoconto incontro del 4/06/2024 con i rappresentanti del Garante per la protezione dei dati personali).
7 Doc. n. 17 (Integrazione memoria e presentazione impegni - prot. n. 0057877 del 7/06/2024).
8 Doc. n. 20 (Trasmissione documentazione - prot. 0060366 del 14/06/2024).
9 Doc. n. 22 (Verbale dell'audizione di Poste Italiane del 18/06/2024).
10 Doc. n. 25 (Risposta alla richiesta di informazioni formulata in audizione - prot. n. 0071297 del 18/07/2024).
11 Doc. n. 29 (Comunicazione di rigetto degli impegni - prot. n. 0083812 del 10/09/2024).
12 Doc. n. 31 (Resoconto incontro del 19/09/2024 con i rappresentanti del Garante per la protezione dei dati personali).
13 Doc. n. 34 (Resoconto incontro del 23/09/2024 con i rappresentanti del Garante per la protezione dei dati personali e Banca d'Italia).
14 Doc. n. 33 (Richiesta di informazioni - prot. n. 0088738 del 26/09/2024).
15 Doc. n. 35 (Risposta alla richiesta di informazioni - prot. n. 0094240 del 17/10/2024).
16 Doc. n. 36 (Integrazione risposta alla richiesta di informazioni - prot. n. 0095339 del 23/10/2024).

nell'ambito dei plessi normativi di rispettiva competenza, in relazione alla condotta posta in essere da Poste Italiane, ribadendo l'opportunità di garantire un processo condiviso e coordinato[17].

14. In data 11 novembre 2024, Poste Italiane, dietro sua istanza, è stata nuovamente sentita in audizione[18] e, nel corso della stessa, il Professionista ha presentato una nuova proposta di impegni, ai sensi dell'articolo 27, comma 7, del Codice del consumo, volti a rimuovere i profili di scorrettezza della condotta oggetto di contestazione, che l'Autorità ha esaminato e, nell'adunanza del 17 dicembre 2024, ne ha deliberato il rigetto per l'interesse a procedere all'accertamento dell'eventuale infrazione, in considerazione della rilevanza dei diritti dei consumatori sui quali incidono le condotte del Professionista[19].

15. In data 14 gennaio 2025, si è svolto un ulteriore incontro in cui gli Uffici hanno aggiornato i rappresentanti del GPDP sullo stato del procedimento[20].

16. In data 17 gennaio 2025, il Professionista ha comunicato l'intenzione di rimuovere il blocco delle *App* di Poste Italiane entro la fine del mese di febbraio 2025[21], secondo le modalità informatiche e tecniche indicate con successiva comunicazione del 27 gennaio 2025[22].

17. In data 18 febbraio 2025, è stata comunicata alla Parte la conclusione della fase istruttoria ai sensi dell'articolo 17, comma 1, del Nuovo Regolamento attraverso la comunicazione di contestazione degli addebiti ed è stato assegnato un termine di venti giorni per eventuali controdeduzioni scritte in replica, da presentarsi al Collegio[23].

18. In data 25 febbraio 2025, Poste Italiane ha presentato istanza di audizione finale dinanzi al Collegio[24].

19. In data 4 marzo 2025, il Professionista ha comunicato di aver rimosso, a far data dal 18 febbraio 2025, il blocco delle *App* Banco Posta e PostePay, per gli utenti che decidono di non rilasciare/confermare l'autorizzazione richiesta per i presidi antifrode[25].

20. In data 5 marzo 2025, è stato comunicato al Professionista che il Nuovo Regolamento non prevede lo svolgimento di un'audizione dinanzi al Collegio e che, al fine di garantire compiutamente il contraddittorio di fronte all'organo decidente e i diritti di difesa, la Parte avrebbe potuto presentare direttamente al Collegio controdeduzioni scritte in replica agli addebiti contestati con la sopracitata comunicazione di contestazione degli addebiti, trasmessa in data 18 febbraio 2025[26], ai sensi dell'articolo 17, comma 1, del richiamato Nuovo Regolamento.

---

17 Doc. n. 34 (Resoconto incontro del 7/10/2024 con i rappresentanti del Garante per la protezione dei dati personali e Banca d'Italia).

18 Doc. n. 40 (Verbale dell'audizione di Poste Italiane dell'11/11/2024).

19 Doc. n. 42 (Comunicazione di rigetto degli impegni - prot. n. 0110911 del 18/12/2024).

20 Doc. n. 45 (Resoconto incontro del 14/01/2025 con i rappresentanti del Garante per la protezione dei dati personali).

21 Doc. n. 47 (Arrivo informazioni - prot. n. 0003542 del 17/01/2025).

22 Doc. n. 48 (Arrivo informazioni - prot. n. 0005408 del 27/01/2025).

23 Doc. n. 59 (Comunicazione di contestazione degli addebiti - prot. n. 0011880 del 18/02/2025).

24 Doc. n. 60 (Istanze di audizione dinnanzi al Collegio e di accesso agli atti - prot. n. 0014175 del 25/02/2025).

25 Doc. n. 61 (Arrivo informazioni- prot. n. 0016063 del 5/03/2025).

26 Doc. n. 62 (Comunicazione esito istanza richiesta audizione - prot. n. 0016191 del 5703/2025).

21. In data 10 marzo 2025[27], è stata depositata la memoria conclusiva del Professionista, successivamente integrata in data 12 marzo 2025[28].

22. Poste Italiane ha esercitato il diritto di accesso agli atti del fascicolo in base alle istanze del 27 gennaio 2025[29] e 25 febbraio 2025[30] che sono state accolte con la trasmissione della documentazione accessibile rispettivamente in data 6 febbraio 2025[31] e 10 marzo 2025[32].

23. In data 13 marzo 2025, è stata trasmessa la richiesta di parere alla Banca d'Italia[33], ai sensi dell'articolo 27, comma 1-*bis*, del Codice del consumo, nonché all'Autorità per le Garanzie nelle Comunicazioni (di seguito, "AGCOM")[34], ai sensi dell'articolo 27, comma 6, del Codice del consumo.

24. In data 13 marzo 2025, inoltre, in considerazione della specificità del caso, è stato richiesto un parere al GPDP[35].

25. In data 2 aprile 2025, è stato comunicato alla Parte il cambio del funzionario responsabile[36].

26. In data 2 aprile 2025, è pervenuto il parere di Banca d'Italia[37], il 14 aprile 2025 quello del GPDP[38] e il 15 aprile 2025, quello dell'AGCOM[39].

III.2. Le risultanze istruttorie

27. Il procedimento trae origine dalle segnalazioni, ricevute da parte di alcuni consumatori a partire dal mese di aprile 2024, relative all'operato del Professionista.

28. In particolare, dalla documentazione agli atti è emerso che, a partire dai primi giorni del mese di aprile 2024, i titolari di rapporti Banco Posta e PostePay che utilizzano i servizi tramite le relative *App* sul proprio *smartphone* con sistema operativo Android, hanno ricevuto in occasione dell'apertura delle suddette *App*, il seguente messaggio: "*Proteggi il tuo dispositivo. Al fine di prevenire potenziali frodi e assicurarti un'esperienza ancora più sicura nell'utilizzo delle sue applicazioni, Poste Italiane introduce un nuovo presidio di sicurezza. Clicca sul bottone «Vai alle impostazioni» e autorizza l'App Poste Italiane ad accedere ai dati per rilevare la presenza di eventuali software dannosi.* ***La funzionalità è obbligatoria, attivala subito****.* ***In assenza di tale***

---

27 Doc. n. 66 (Memoria conclusiva - prot. n. 0017558 del 10/03/2025).

28 Doc. n. 67 (Integrazione memoria conclusiva - prot. n. 0018034 del 12/03/2025).

29 Doc. n. 49 (Istanza di accesso agli atti - prot. n. 0005776 del 27/01/2025).

30 Doc. n. 60 (Istanze di audizione dinnanzi al Collegio e di accesso agli atti - prot. n. 0014175 del 25/02/2025).

31 Doc. n. 57 (Esito istanza accesso agli atti e trasmissione documentazione - prot. n. 0008646 del 6/02/2025).

32 Doc. n. 65 (Esito istanza accesso agli atti e trasmissione documentazione - prot. n. 0017432 del 10/03/2025).

33 Doc. n. 68 (Richiesta parere Banca d'Italia - prot. n. 0018436 del 13/03/2025) e Doc. n. 71 (Trasmissione documentazione Banca d'Italia - prot. n. 0018698 del 14/03/2025).

34 Doc. n. 70 (Richiesta parere Autorità per le Garanzie nelle Comunicazioni - prot. 0018433 del 13/03/2025) e Doc. n. 72 (Trasmissione documentazione Autorità per le Garanzie nelle Comunicazioni - prot. n. 0018690 del 14/03/2025).

35 Doc. n. 69 (Richiesta parere Garante per la protezione dei dati personali - prot. n. 0018438 del 13/03/2025).

36 Doc. n. 74 (Comunicazione cambio funzionario responsabile prot. 0024534 del 2/04/2025).

37 Doc. n. 73 (Parere Banca d'Italia - prot. 0024219 del 02/04/2025).

38 Doc. n. 76 (Parere Garante Privacy - prot. 0027999 del 14/04/2025).

39 Doc. n. 77 (Parere AGCOM - prot. 0028336 del 15/04/2025).

autorizzazione hai a disposizione un numero massimo di 3 accessi dopo i quali non ti sarà più possibile accedere e operare in App"[40].

29. Cliccando sul pulsante ipertestuale "*Vai alle impostazioni*", si accedeva alla sezione delle impostazioni del sistema operativo Android, in cui poteva essere fornito il proprio consenso affinché le *App* di Poste Italiane possano accedere ai "*Dati di utilizzo*"[41]. Relativamente a questi ultimi, il sistema operativo Android fornisce agli utenti messaggi, da cui emerge una portata molto ampia dell'autorizzazione richiesta, del seguente tenore: "*l'accesso ai dati di utilizzo consente ad un'App di controllare quali altre App utilizzi e con quale frequenza, oltre a informazioni come operatore, lingua impostata e altri dettagli*" (cfr. Immagine 2)[42], ovvero, informando che fornendo l'autorizzazione "*consentite alle applicazioni di monitorare quali altre applicazioni utilizzate, e con quale frequenza, e di identificare il gestore telefonico, le indicazioni relative alla lingua e altri dati di utilizzo*"[43].

[40] Doc. n. 2, all. 2 (Segnalazione - prot. n. 37248 dell'8/04/2024) e Doc. n. 4, all. 1 (Segnalazione - prot. 0038052 del 10/04/2024).

[41] Per dati di utilizzo (in inglese *usage data* o *usage stats*) si intendono le informazioni tecniche raccolte da un'*App* o da un sistema operativo su come viene usato il dispositivo o le applicazioni installate.

[42] Doc. n. 12, all. 1 (Segnalazione - prot. 47462 del 10/05/2024).

[43] Doc. n. 2, all. 1 (Segnalazione - prot. 37248 dell'8/04/2024).

Immagine 1

Immagine 2

30. L'utente che non concedeva l'autorizzazione ad accedere ai dati dello *smartphone*, cliccando su "*Non ora*" (cfr. Immagine 1), poteva operare sull'App soltanto per ulteriori tre volte (divenute cinque a partire dal 4 luglio 2024[44]). Una volta superato il numero di accessi consentiti, senza aver concesso l'autorizzazione come richiesto nel messaggio, infatti, l'App si bloccava. Se l'utente provava un nuovo accesso, l'App non si attivava, impedendogli di usufruire dei relativi servizi; contestualmente il consumatore veniva invitato nuovamente a modificare le impostazioni del proprio cellulare autorizzando l'App ad accedere ai dati dello stesso (cfr. Immagine 3).

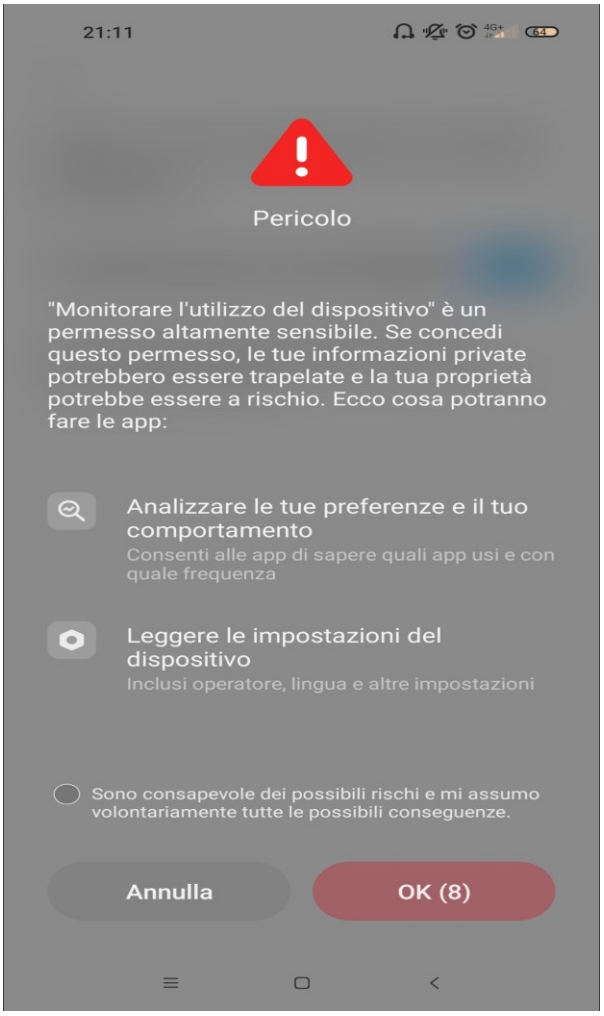
31. Tra le segnalazioni ricevute, un consumatore ha riportato che, durante la procedura di autorizzazione, è apparso il seguente messaggio[45] (cfr. Immagine 4).

[44] Doc. n. 25 (Risposta alla richiesta di informazioni formulata in audizione - prot. 0071297 del 18/07/2024).

[45] Doc. n. 12, all. 2 (Segnalazione – prot. 0047642 del 10/05/2024).

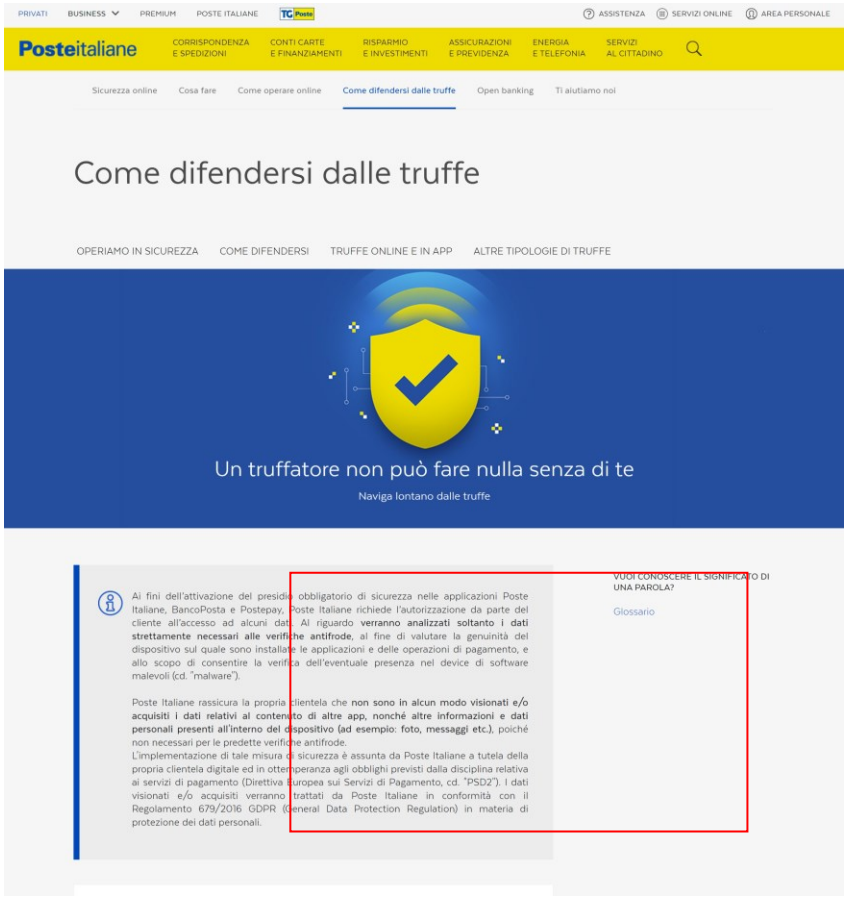
Immagine 3

Immagine 4



32. Inoltre, dalla documentazione in atti risulta che, cliccando sul *link* ipertestuale "*scopri di più*", presente in fondo all'avviso, si veniva indirizzati alla sezione del sito *web* di Poste Italiane in cui, nel descrivere le truffe *online* e i modi per difendersi da esse, era genericamente indicato che "*ai fini dell'attivazione del presidio obbligatorio di sicurezza, nelle applicazioni Poste Italiane, Banco Posta e PostePay, Poste Italiane richiede l'autorizzazione da parte del cliente all'accesso ad alcuni dati*" senza, tuttavia, specificare le tipologie di dati interessati all'accesso (cfr. Immagine 5).

Immagine 5



33. In particolare, i segnalanti hanno lamentato l'ampia portata dell'autorizzazione richiesta[46], che avrebbe consentito a Poste Italiane l'accesso a una pluralità di dati personali, oltre che il monitoraggio dell'eventuale utilizzo, da parte dell'utente, di *App* di operatori concorrenti, nonché la scarsità e vaghezza delle informazioni fornite dal Professionista per giustificare tale richiesta[47].

[46] Cfr. Doc. n. 3 (Segnalazione - prot. n. prot. 37250 dell'8/04/2024). Il segnalante infatti lamenta che: "*se da impostazioni si controllano però i consensi (obbligatori) forniti, di fatto, una volta che si è dato il consenso (obbligatorio) si scopre che i dati che rendiamo «visibili» a Poste sono davvero tanti: ad esempio, si autorizza la App PostePay e Banco Posta a monitorare l'attività di altre App installate sul telefono (comprese quindi quelle per l'*home banking *di altri istituti bancari o carte di credito loro competitors) con quale frequenza le utilizziamo, e quale sia il nostro gestore telefonico (ovvero riveliamo a Poste, che gestisce l'operatore Poste Mobile, di quale suo concorrente siamo clienti)*".

[47] Cfr. Doc. n. 8 (Segnalazione - prot. n. 41365 del 22/04/2024), in cui il segnalante lamenta: "*Ulteriore aggravante è il fatto che se si cerca di approfondire la questione si possono consultare solamente informazioni vaghe e per nulla specifiche. Tutto ciò a mio avviso è inaccettabile e rappresenta una gravissima violazione della* privacy *e della proprietà privata*".

34. I consumatori hanno, altresì, contestato l'obbligatorietà della richiesta di autorizzazione, in considerazione del fatto che, in caso di mancato rilascio, era impossibile continuare a utilizzare le *App*[48].

35. Nel corso dell'audizione tenutasi in data 18 giugno 2024, la Società ha chiarito che il sistema antifrode introdotto con le modalità sopra descritte ha interessato solo i clienti che utilizzano dispositivi Android. Quanto alle modalità di funzionamento della componente *anti malware* di tale sistema, su richiesta degli Uffici, è stato precisato che la stessa opera effettuando l'analisi non solo delle applicazioni installate sui dispositivi ma anche di quelle c.d. *running*, vale a dire le *App* che risultano in esecuzione quando è in corso l'utilizzo delle applicazioni di Poste Italiane sullo *smartphone* interessato.

36. A tale riguardo, il Professionista ha inizialmente asserito che la normativa antifrode richiederebbe "*di effettuare analisi specifiche, utilizzando* […] *informazioni tipicamente attestate sul dispositivo che il cliente sta utilizzando,* […]", affermando, altresì, che: "*al fine di poter efficacemente ottemperare a tali obblighi normativi che hanno la finalità di garantire la sicurezza dei sistemi di pagamento per il pubblico si rende necessario raccogliere le informazioni oggetto dell'avviso pubblicato sulle App*"[49].

37. *[Omissis]*[*].

38. L'istruttoria ha posto anche in rilievo che la condotta oggetto di accertamento ha interessato diversi milioni di consumatori[50]. In particolare, nel periodo 1° maggio 2024 - 30 giugno 2024[51] (cfr. Tabella 1), risulta che a un numero estremamente elevato di *App* Banco Posta e PostePay[52] (pari a quasi *[5-10]* milioni) è stato richiesto di fornire l'autorizzazione ad accedere ai dati dello *smartphone* su cui erano installate le relative *App*, per poter continuare a usufruire delle stesse per la gestione dei propri pagamenti o risparmi. Inoltre, è stato bloccato un numero elevato di *App* (complessivamente pari a *[250.000-500.000],* corrispondenti ai consumatori che non hanno fornito l'autorizzazione richiesta. Altri utenti titolari di *App* (complessivamente pari a *[750.000-1.000.000],* invece, si sono visti comunque limitare fortemente le possibilità di utilizzo delle *App* dei propri conti correnti, in quanto è stato circoscritto a tre il numero di accessi consentiti dopo i quali sarebbero stati costretti a scegliere tra fornire l'autorizzazione o subire il blocco delle *App*. Infine, risulta che, un numero particolarmente elevato di consumatori (pari a circa *[5.000.000-10.000.000])* che avevano installato le *App* Banco Posta e PostePay ha fornito il proprio consenso all'accesso ai propri dati.

---

[48] Doc. n. 4 (Segnalazione - prot. n. 38052 del 10/04/2024), in cui il segnalante lamenta che "[…] *a fronte di tale intimazione non è fornita indicazione circa modalità alternative o sostitutive dell'App PostePay*".

[49] Doc. 14 pag. 4.

[*] Nella presente versione alcuni dati sono omessi, in quanto si sono ritenuti sussistenti elementi di riservatezza o di segretezza delle informazioni.

[50] Doc. 14, cit. pag. 17.

[51] Doc. n. 25 cit., pag. 4.

[52] Al riguardo, il Professionista ha precisato che risulta impossibile fornire il numero degli utenti a causa della possibilità che ciascuno di essi sia dotato di più *device* e che il rilascio dell'autorizzazione abbia riguardato una sola delle due *App* di cui è titolare (cfr. Doc. n. 25, cit. e Doc. n. 35, cit.).

Tabella 1

	App BP		*App* PP	
	Numero	%	*Numero*	%
***App* Bloccate**	*[100.000-150.000]*	*[1-5%]*	[*150.000-200.000]*	*[1-5%]*
***App* non bloccate ma che ancora non hanno fornito autorizzazione** (non avendo effettuato il numero di accessi massimo, pari a 3 nel periodo in esame)	*[100.000-500.000]*	*[5-10%]*	*[200.000-600.000]*	*[5-10%]*
***App* che hanno fornito autorizzazione**	*[1.000.000-5.000.000]*	[85-90%]	*[1.000.000-5.000.000]*	[85-90%]
Totale *App*	*[1.000.000-5.000.000]*	*[95-100%]*	*[5.000.000-10.000.000]*	*[95-100%]*

39. Nel periodo 1° maggio 2024 - 30 settembre 2024[53](cfr. Tabella 2), a seguito dell'innalzamento del numero di accessi da tre a cinque prima di bloccare l'operatività delle *App* a coloro che non fornivano l'autorizzazione - disposto dal Professionista a partire dal 4 luglio 2024 - il numero di *App* rispetto alle quali non è stata fornita l'autorizzazione è rimasto elevato (pari a circa *[1.500.000-2.500.000];* pertanto, coloro che non avevano fornito l'autorizzazione in precedenza hanno, comunque, continuato a non fornirla anche a seguito dell'innalzamento del numero di accessi consentito. Il numero di *App* bloccate perché non è stata rilasciata l'autorizzazione richiesta, è risultato pari a *[100.000-200.000],* mentre quello relativo alle *App* per le quali è stata rilasciata la predetta autorizzazione è stato pari a *[7.500.000-15.000.000].* Inoltre, il numero delle *App* Banco Posta e PostePay interessate dalla richiesta di autorizzazione è risultato aumentato (oltre *[10-15]* milioni)[54].

[53] Doc. n. 35, cit. pag. 1.

[54] Il Professionista ha successivamente comunicato che tale dato ha subito un aumento di circa *[1-5]* milioni (Doc. n. 35, cit. pag. 3).

Tabella 2

	***App* BP**		***App* PP**	
	numero	*%*	*numero*	*%*
***App* Bloccate**	*[50.000-100.000]*	*[1-5%]*	*[100.000-150.000]*	*[1-5%]*
***App* non bloccate ma che ancora non hanno fornito autorizzazione** (non avendo effettuato il numero di accessi massimo)	*[500.000-1.000.000]*	*[10-15%]*	*[1.000.000-5.000.000]*	*[10-15%]*
***App* che hanno fornito autorizzazione**	*[1.000.000-5.000.000]*	*[80-85%]*	*[5.000.000-10.000.000]*	*[80-85%]*
Totale *App*	[5.000.000-*10.000.000]*	*[95-100%]*	*[5.000.000-10.000.000]*	*[95-100%]*

40. In relazione al numero di *alert* o di *[omissis],* indicativo del rischio di frode connesso alle operazioni compiute dagli utenti di Poste, dalla documentazione in atti, risulta che, nel bimestre precedente l'implementazione delle nuove misure di sicurezza, il sistema antifrode adottato dal Professionista ha rilevato circa *[50.000-100.000] alert* per *malware*; mentre, a seguito dell'introduzione del nuovo sistema antifrode, lo stesso ha rilevato circa *[10.000-50.000] alert* per *malware*, di cui *[5.000-10.000] alert* collegati ad *App* in stato "*running*" sui *device* Android (cfr. Tabella 3)[55].

Tabella 3

	Ottobre 2023 - Marzo 2024	**Aprile 2024 - Ottobre 2024**
i) numero di alert o score che indicano il rischio di frode ricevuti	**Circa *[50.000-100.000]*** Il dato è indicativo tuttavia dei soli due mesi febbraio/marzo 2024, in quanto la rilevazione degli eventi malware, secondo quanto indicato dal Professionista, è stata effettivamente attivata a fine gennaio 2024.	**Circa *[10.000-50.000]***
di cui alert rilevati per effetto delle informazioni derivanti dal monitoraggio delle *App* in esecuzione	n.a.	Circa ***[5.000-10.000]***
ii) percentuali di "*falsi positivi*" rispetto al dato di cui al punto i)	*[95-100%]*	*[95-100%]*

[55] Doc. n. 36, pag. 2 cit..

41. In data 18 luglio 2024[56], Poste Italiane ha comunicato di aver spontaneamente apportato miglioramenti all'informativa resa ai consumatori sul sito www.poste.it, accessibile anche tramite il predetto *link* ipertestuale "*scopri di più*", chiarendo la finalità dell'autorizzazione richiesta, le alternative a disposizione della clientela, e di aver incrementato da tre a cinque il numero di accessi a disposizione del cliente, durante i quali lo stesso può scegliere se concedere o meno l'autorizzazione all'accesso ai dati richiesti.

42. In data 5 marzo 2025[57], la Società ha dato conto di aver adottato, a far data dal 18 febbraio 2025, una serie di misure correttive e ripristinatorie, prevedendo interventi a tutela dei consumatori interessati dal blocco e consentendo di confermare/revocare la propria scelta anche a coloro che avevano già fornito il consenso. In tal modo, Poste Italiane ha rinunciato al blocco delle *App* degli utenti di Banco Posta e PostePay che non forniscono l'autorizzazione al monitoraggio del proprio dispositivo, avendo cura di precisare che avrebbe assicurato in ogni caso un sistema di protezione dalle frodi informatiche anche a tale categoria di consumatori.

43. In particolare, Poste Italiane ha modificato il proprio *modus operandi*, consentendo:

- a coloro che avevano già fornito l'autorizzazione al monitoraggio del proprio *smartphone*, di confermare o revocare la propria autorizzazione, potendo in ogni caso continuare a operare sull'App anche in caso di revoca della stessa;
- ai clienti che non avevano ancora rilasciato l'autorizzazione (compresi coloro che ancora non avevano effettuato i cinque accessi consentiti) di decidere se fornire o meno la stessa, potendo in ogni caso accedere alle *App* a prescindere dalla scelta effettuata;
- ai clienti che avevano negato la propria autorizzazione, ai quali era stato inibito l'accesso alle *App*, avendo esaurito tutti gli accessi a disposizione, di poter nuovamente utilizzare le *App*, senza dover prestare necessariamente il consenso.

44. In caso di mancato consenso, al consumatore è stato, inoltre, consentito di scegliere di non visualizzare il messaggio all'apertura dell'App con cui si richiede l'autorizzazione cliccando sul tasto "*Non mostrare più*", presente nella schermata.

45. Il Professionista ha, altresì, comunicato di aver, alla medesima data del 18 febbraio 2025, adeguato la relativa informativa presente sul proprio sito *web*, dando conto della possibilità di utilizzare le *App* anche in assenza della predetta autorizzazione.

IV. LE ARGOMENTAZIONI DIFENSIVE DEL PROFESSIONISTA

46. Poste Italiane ha risposto alla richiesta di informazioni contenuta nella comunicazione di avvio del procedimento e illustrato le argomentazioni difensive sia nel corso delle due audizioni svolte con gli Uffici istruttori[58] che tramite le memorie pervenute nel corso del procedimento nelle date 13

[56] Doc. n. 25, cit..
[57] Doc. n. 61, cit..
[58] Doc. n. 22, cit. e Doc. n. 40., cit..

maggio 2024[59], 6 giugno 2024[60], 18 luglio 2024[61], 17 ottobre 2024[62], 22 ottobre 2024[63], 17 gennaio 2025[64], 27 gennaio 2025[65], 5 marzo 2025[66], nonché attraverso le controdeduzioni presentate al Collegio in replica alla contestazione degli addebiti del 10 marzo 2025[67], integrate in data 12 marzo 2025[68].

47. La Parte ha, inoltre, sottolineato che l'implementazione di una piattaforma antifrode - rientrando nel quadro delle iniziative riconducibili a previsioni e obblighi derivanti dalla normativa di settore - risponderebbe all'esigenza di proteggere i propri clienti da eventuali frodi e migliorare la loro soddisfazione. Per tale motivo, Poste ha dichiarato di aver agito in stretta e diretta applicazione della normativa in materia di servizi di pagamento e nel rispetto della normativa in materia di protezione dei dati personali[69].

48. In particolare, secondo il Professionista, il comportamento adottato deriverebbe dall'esigenza di rispettare le prescrizioni normative contenute nella Direttiva UE 2015/2366 (c.d. "PSD2") e negli *Standard* Tecnici di Regolamentazione (di seguito anche "RTS"), elaborati dall'EBA e adottati con il Regolamento (UE) 2018/389, che ha reso obbligatorio "*per i prestatori di servizi di pagamento il rispetto degli* standard *tecnici che disciplinano la sicurezza delle transazioni* online" e, in particolare, gli articoli 2 e 18 delle RTS, nonché per dare seguito alle indicazioni ricevute dalle Autorità di settore[70].

49. Poste Italiane ha, inoltre, fatto presente di aver introdotto il nuovo sistema di monitoraggio solo sugli *smartphone* con sistema operativo Android, precisando che gli avvisi oggetto delle segnalazioni sono stati introdotti a partire dal 3 aprile 2024 e hanno interessato esclusivamente i sistemi Android più recenti (non anche quelli più datati)[71].

50. Al riguardo, la Società ha giustificato l'adozione della misura per i soli utenti Android in considerazione della natura "aperta" del sistema (c.d. *open-source*) e, dunque, potenzialmente più vulnerabile, che necessiterebbe dell'impiego di un *feed anti-malware* per mettere maggiormente in sicurezza le operazioni effettuate dalla clientela tramite *App*. Diversamente, per quanto riguarda i

---

59 Doc. n. 14, cit..
60 Doc. n. 17, cit..
61 Doc. n. 25, cit..
62 Doc. n. 35, cit..
63 Doc. n. 36, cit..
64 Doc. n. 47, cit..
65 Doc. n. 48, cit..
66 Doc. n. 61, cit..
67 Doc. n. 66, cit..
68 Doc. n. 67, cit..
69 Doc. nn. 14 e 22, cit..
70 Doc. 14 cit., pagg. 2 e 3.
In particolare, il Professionista dichiara che "*La normativa quindi richiede ai Prestatori di servizi di pagamento 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.*" (cfr. pag. 4 doc. 14, cit.).
71 Doc. 14, cit., pag. 17 e Doc. 22, cit. pag. 2.

sistemi IOS "*essi costituiscono un «ecosistema monolitico» e nativamente già prevedono strumenti* anti-malware *integrati, a differenza dei sistemi Android che vengono personalizzati in maniera differente dai vari produttori dei* device."[72]. In merito alla mancata introduzione di analoghi sistemi antifrode per l'accesso ai servizi della Società tramite PC, la Parte ha affermato che "*l'applicativo non è tecnicamente integrabile nel* browser *del cliente - il quale non è prodotto da Poste - poiché, pur girando all'interno del sistema operativo del* device*, non consente di controllare altri programmi sul* device *stesso per attività* anti-malware*. In ogni caso, giova rappresentare che i* browser *più noti sul mercato possono essere considerati tendenzialmente sicuri in quanto bloccano nell'immediato attività non autorizzate di terzi, rendendo la navigazione Internet particolarmente affidabile*." [73].

51. Il Professionista ha, inoltre, chiarito che il sistema antifrode scelto[74] - basato su modelli analitico-predittivi relativi al comportamento degli utenti, anche grazie all'adozione dello specifico applicativo *anti malware* - analizza il comportamento dei consumatori (*customer* behaviour) secondo un approccio *risk based*, valutando l'integrità delle applicazioni presenti sul dispositivo e rilevando la presenza di eventuali *malware* o tecnologie di *jailbreak/root*[75], tramite l'elaborazione di un indice di rischio delle transazioni[76].

52. I dati riferiti alle *App* in esecuzione verrebbero raccolti in forma anonimizzata (ai nomi in chiaro delle applicazioni in esecuzione e ai dati a esse correlati come elementi multimediali, dati personali, etc., verrebbe, infatti, attribuito un codice *hash*[77] in MD5, dal quale non sarebbe possibile ricavare informazioni personali) e suddivisi per classi di rischio.

53. I dati così acquisiti, a dire di Poste Italiane, sarebbero "*monitorati in forza di un obbligo di legge*" e sarebbero utilizzati esclusivamente per finalità antifrode e non per finalità commerciali, essendo irreversibilmente anonimizzati e conservati in modalità segregate (sia dal punto di vista logico che

---

[72] Doc. n. 35, cit. pag. 2.

[73] Doc. n. 35, cit. pag. 2. Poste Italiane dichiara "*A titolo esemplificativo, Chrome - come dichiarato da Google - "è progettato per essere sicuro e ti protegge da siti pericolosi e ingannevoli che potrebbero carpire le tue password o infettare il tuo* computer*. Tecnologie avanzate quali isolamento dei siti, sandboxing e protezione preventiva dal phishing proteggono te i tuoi dati.*".

[74] Doc. n. 22, pagg. 1-2 (Verbale dell'audizione di Poste Italiane del 18/06/2024 - prot. 0066773 del 4/07/2024).

[75] Con *jailbreak/root* si intendono le procedure che permettono di ottenere controlli privilegiati su *smartphone* e/o tablet, che consentendo tra l'altro l'installazione di applicazioni e la modifica di *file* di sistema.

[76] Doc. n. 35, pagg. 6-7 (Risposta alla richiesta di informazioni prot. 0094240 del 17/10/2024).

[77] Per codice *hash* si intende una stringa di caratteri generata da una funzione matematica chiamata funzione di *hash*. Questa funzione prende un *input* (può essere un *file*, una *password*, un testo, ecc.) e produce un *output* di lunghezza fissa che rappresenta una sorta di "*impronta digitale*" dell'input. L'impronta *hash* di un testo o di un *file* informatico è una sequenza di lettere (a, b, c, d ed f) e cifre (da zero a nove), ottenuta applicando un particolare algoritmo di calcolo alla sequenza di *bit* che formano il testo o il *file*.
Un codice *hash* presenta le seguenti caratteristiche:

1. Lunghezza fissa: indipendentemente dalla dimensione dell'*input*, l'*hash* ha sempre la stessa lunghezza (es. 64 caratteri per SHA-256).
2. Deterministico: lo stesso input genera sempre lo stesso *hash*.
3. Non invertibile: è praticamente impossibile risalire all'*input* originale partendo dall'*hash* (per una buona funzione di *hash*).
4. Sensibile alle modifiche: anche un piccolo cambiamento nell'input produce un *hash* completamente diverso.
5. Unico (idealmente): due input diversi non dovrebbero mai generare lo stesso *hash* (collisione).

fisico) su piattaforma tecnologica antifrode del tutto distinta dalle altre, incluse quelle contenenti dati utilizzabili per finalità commerciali[78].

54. Tale segregazione e l'assenza di qualsivoglia natura economica della scelta del cliente in ordine al rilascio della predetta autorizzazione, ad avviso del Professionista, escluderebbero la configurabilità della condotta come "*pratica commerciale tanto più come scorretta e aggressiva*" dal momento che "*i dati raccolti in fase di accesso alle App vengono trattati esclusivamente a tutela dell'utenza da potenziali frodi, e non vengono trattati per finalità diverse, tanto meno commerciali e, pertanto, non assumono in alcun modo valenza economico/commerciale*"[79].

55. Nello specifico, il sistema adottato dalla Società sarebbe in grado di eseguire le seguenti funzioni sui dispositivi in cui sono in esecuzione le *App* di Poste Italiane: ***(i)*** identificazione del dispositivo (*i.e.* versione del sistema operativo, aggiornamenti di sicurezza, versione delle *App* Poste, tipologia d'interfaccia *web* del dispositivo etc.); ***(ii)*** localizzazione del dispositivo attraverso la funzionalità GPS e altri dati correlati; ***(iii)*** verifica dell'integrità del dispositivo (*i.e.* eventuale processi di *jailbreaking/rooting*); ***(iv)*** *anti malware,* sia in relazione alle *App* installate che su quelle *running*.

56. Con riferimento ai dati relativi al numero di *alert* per *malware* registrati nel bimestre precedente all'implementazione delle nuove misure - pari a circa *[50.000-100.000]* - che a seguito dell'introduzione del nuovo sistema antifrode (periodo aprile 2024 - ottobre 2024) è risultato pari a *[1.000-50.000],* il Professionista, su richiesta degli Uffici, ha argomentato che l'elevato numero di *alert* che caratterizza il bimestre precedente all'introduzione della misura è da ricondurre a fattori esogeni, riconducibili a generici "*significativi attacchi informatici*", senza, tuttavia, fornire evidenze al riguardo[80]. A questo proposito, la Parte ha evidenziato che l'efficacia della misura deve essere *[omissis]*[81].

57. Relativamente alla contestazione circa l'assenza di alternative disponibili per il consumatore una volta esaurito il numero di accessi per i quali non è richiesta l'autorizzazione ai dati del proprio *smartphone*, Poste Italiane ha rappresentato che "*in ogni caso, il cliente può sempre disporre di canali alternativi, sia fisici (*i.e. *Ufficio Postale) sia digitali (es. sito* web *che risulta accessibile anche attraverso dispositivo mobile), attraverso i quali è possibile effettuare le medesime operazioni nonché accedere alle stesse funzionalità disponibili nelle App*."[82].

58. Il Professionista, a giustificazione del proprio operato, ha affermato, altresì, che l'informativa resa ai consumatori non sia in realtà riconducibile a Poste Italiane e, che pertanto, la Società non avrebbe alcun potere di controllo sul suo contenuto, essendo di esclusiva competenza dei produttori dei dispositivi dotati del sistema operativo Android, precisando che "*tuttavia, nella piena volontà di rendere ancor più approfondita la consapevolezza del cliente sul punto* […] *ha inserito un* link *ipertestuale «scopri di più» immediatamente dopo la spiegazione della richiesta di acquisizione (e prima dell'opzione «Vai alle impostazioni» attraverso la quale l'utente prosegue nel rilascio dell'autorizzazione*)."[83].

---

[78] Doc. 14, cit. pag. 4.
[79] Doc. n.14, cit., pag. 6.
[80] Doc. n. 25, cit., pag. 3 e Doc. n. 36, cit. pag. 2.
[81] Doc. n. 40, cit. pag. 4.
[82] Doc. n. 14, cit..
[83] Doc. n.14, cit..

59. Poste Italiane ha dichiarato, inoltre, che il contenuto del messaggio presente nel predetto *link* "*scopri di più*" - contrariamente a quanto sostenuto dall'Autorità - sarebbe stato, in ogni caso esaustivo e completo, contenendo sia l'indicazione della finalità sottesa al trattamento che la tipologia dei dati[84] (il messaggio era il seguente: "*Ai fini dell'attivazione del presidio obbligatorio di sicurezza, nelle applicazioni Poste Italiane, Banco Posta e PostePay, Poste Italiane richiede l'autorizzazione da parte del cliente all'accesso ad alcuni dati. Al riguardo* ***verranno analizzati soltanto i dati strettamente necessari alle verifiche antifrode****, al fine di valutare la genuinità del dispositivo sul quale sono installate le applicazioni e delle operazioni di pagamento, e allo scopo di consentire la verifica dell'eventuale presenza nel device di* software *malevoli (c.d. «*malware*»).*
Poste Italiane rassicura la propria clientela che ***non sono in alcun modo visionati e/o acquisiti i dati relativi al contenuto di altre App, nonché altre informazioni e dati personali presenti all'interno del dispositivo (ad esempio: foto, messaggi etc****.), poiché non necessari per le predette verifiche antifrode.*
*L'implementazione di tale misura di sicurezza è assunta da Poste Italiane a tutela della propria clientela digitale e in ottemperanza agli obblighi previsti dalla disciplina relativa ai servizi di pagamento (Direttiva Europea sui Servizi di Pagamento, c.d. «PSD2»). I dati visionati e/o acquisiti verranno trattati da Poste Italiane in conformità con il Regolamento 679/2016 GDPR (*General Data Protection Regulation *in materia di protezione dei dati personali*".).
60. Più in generale, anche relativamente alla contestazione circa la contrarietà della condotta al principio generale della diligenza professionale di cui all'articolo 20 del Codice del consumo, la Società ha evidenziato che: "*appare evidente, al contrario, che la condotta di Poste sia stata ispirata al massimo rispetto del principio di diligenza professionale, laddove le azioni adottate dalla Società rappresentano in maniera inconfutabile l'impegno assunto dalla stessa nell'implementare tutte le misure più evolute ed efficaci a tutela della sicurezza degli utenti, anche al fine di assolvere gli obblighi discendenti dalla normativa di riferimento*". Ad avviso del Professionista, infatti: "*per assurdo è proprio l'elevato grado di diligenza professionale richiesto ai prestatori di servizi di pagamento a imporre l'adozione delle misure antifrode in cui si colloca la richiesta avanzata da Poste in sede di accesso alle App; a tal riguardo la consolidata giurisprudenza ritiene, infatti, che affinché il prestatore non venga considerato corresponsabile dell'attività fraudolenta registrata, debba dimostrare di aver posto in essere tutte le azioni di controllo idonee a garantire la sicurezza del servizio, nonché richieste dal tenore di diligenza tecnica che gli compete*" e che "*proprio l'implementazione di sistemi e applicativi antifrode […], in conformità con la normativa vigente in materia di pagamenti elettronici, costituisce prova di una diligenza del prestatore di servizi - analoga a quella dell'accorto banchiere - e contribuisce a rendere evitabile il rischio di operazioni di pagamento non riconducibili alla volontà del cliente*"[85].

[84] Doc. n. 14, cit. pag. 13.
[85] Doc. n. 14, cit., pag. 10.

V. CONTRODEDUZIONI DELLA PARTE ALLA COMUNICAZIONE DI CONTESTAZIONE DEGLI ADDEBITI

61. In data 18 febbraio 2025, è stata trasmessa alla Parte la comunicazione di contestazione degli addebiti ed è stato assegnato un termine di venti giorni per eventuali controdeduzioni scritte in replica, da presentarsi al Collegio[86].

62. Con la memoria depositata il 10 marzo 2025[87], Poste Italiane, rinviando alle argomentazioni e difese formulate in precedenza, ha rappresentato al Collegio le seguenti ulteriori argomentazioni difensive.

63. In via preliminare, il Professionista ha ribadito di aver agito nel rispetto degli obblighi previsti dalla predetta Direttiva PSD2 e dagli RTS nonché della normativa in materia di protezione dei dati personali. Tuttavia, nonostante Poste Italiane giustifichi l'adozione del sistema antifrode alla luce delle esigenze di tutela dei consumatori, tenuto conto anche del numero crescente di frodi, diversamente da quanto sostenuto in precedenza, ammette che "*L'art. 2 delle RTS si limita a codificare, coerentemente con gli obiettivi della Direttiva PSD2, un obbligo di risultato, senza regolare il «funzionamento della componente anti malware»(anche perché specificare a livello normativo le modalità di funzionamento dei presidi antifrode renderebbe gli stessi molto più semplici da aggirare*)." [88].

64. Analogamente, la Parte ha asserito che "*Banca d'Italia, in quanto autorità di regolazione, non prescrive - né tantomeno potrebbe prescrivere - l'adozione da parte degli operatori del settore di tecnologie sviluppate da specifici provider: ciò si sostanzierebbe infatti nell'imposizione di un fornitore. Similmente, Banca d'Italia non definisce, con questo grado di dettaglio, le «specifiche caratteristiche» che i sistemi anti-malware devono presentare*."[89].

65. In particolare, i rilievi del Professionista hanno riguardato, in sintesi, i seguenti aspetti:

a. l'assenza della finalità commerciale della pratica. Poste Italiane, infatti, sostiene che il sistema antifrode adottato non avrebbe scopi promozionali o commerciali, né genererebbe patrimonializzazione dei dati degli utenti, anche in considerazione del fatto che i dati sarebbero raccolti in forma anonima (mediante l'attribuzione di un codice *hash MD5*), tramite l'elaborazione di un indice di rischio che non consentirebbe l'identificazione delle relative *App* (installate e in uso sul dispositivo) e che, comunque, tale dato sarebbe trasmesso a una piattaforma segregata, inaccessibile alle divisioni *marketing* o commerciali del Professionista e che, in ogni caso, gli stessi non sono ceduti a terzi;

b. l'inapplicabilità del Codice del consumo. A detta del Professionista non sussisterebbe alcun rapporto di consumo legato alla valorizzazione economica dei dati personali trattati per garantire la funzionalità del sistema anti *malware*[90]. Per tale motivo nel caso di specie, difetterebbero i

---

86 Doc. n. 59, cit..

87 Doc. n. 66, cit..

88 Doc. n. 66, cit. pag. 20.

89 Doc. n. 66, cit. pag. 21.

90 A sostegno delle proprie argomentazioni, il Professionista richiama alcuni precedenti dell'Autorità (cfr. procedimenti nn. PS11150- *ICloud*; PS11147 - *Google Drive Sweep 2017*; PS11112 - *Facebook - Condivisione Dati con Terzi*; PS11710 -*Telepass/Accordo Prima Assicurazione*; PS11149 - *Dropbox*) nonché alcuni riferimenti giurisprudenziali (ad esempio, Corte di Giustizia dell'Unione europea, sentenza del 17 ottobre 2013 C-391/12 - *RLvS*).

presupposti essenziali per l'applicabilità della disciplina consumeristica, in quanto sarebbe assente ogni finalità commerciale e "*scambio di prestazioni*", non potendosi configurare il mero trattamento di dati personali - in assenza di qualsivoglia utilizzo commerciale degli stessi - come controprestazione per un servizio.

c. il rispetto dei principi di buona fede e della diligenza professionale. Come anticipato, Poste Italiane motiva l'adozione del sistema anti *malware* in esame con l'esigenza di rispettare la Direttiva PSD2 e le RTS, nella misura in cui questi impongono ai prestatori di servizi finanziari di dotarsi di presidi antifrode efficaci. Al riguardo, il Professionista, richiamando un precedente dell'Autorità[91], sostiene che l'adozione di presidi antifrode, "*contribuendo a rendere evitabile il rischio di operazioni di pagamento non riconducibili alla volontà del cliente*"[92] costituirebbe prova della diligenza professionale del prestatore di servizi [93];

d. l'assenza dell'aggressività della pratica. Poste Italiane, ribadendo la propria buona fede nell'adozione del sistema antifrode, sostiene, altresì, che la misura del blocco delle *App* sarebbe proporzionata rispetto alle finalità di tutela degli utenti che utilizzano *device*, a suo dire "più vulnerabili" (*i.e.* Android) e disconosce ogni possibile profilo di costrizione/imposizione della propria condotta, anche in considerazione della possibilità riconosciuta agli utenti di effettuare le operazioni tramite *browser* e/o Ufficio postale. Al riguardo, Poste Italiane dichiara, infatti, che il disagio dell'impedimento di accesso all'App paventati dagli Uffici si sarebbe tradotto al più nel "*ritorno a una modalità di autorizzazione delle operazioni di pagamento* online *che costituiva, fino a pochissimi anni fa, l'unica disponibile sul mercato (salvo le precedenti modalità di accesso tramite O-Key) e con la quale il consumatore medio ha già significativa dimestichezza*"[94];

e. la completezza dell'informativa resa. Poste Italiane ribadisce la trasparenza e l'adeguatezza informativa del messaggio di *alert*, con cui veniva richiesta ai consumatori l'autorizzazione ad accedere ai dati del proprio *device*.

f. avvenuta adozione di misure migliorative e ripristinatorie. Infine, la Parte sottolinea l'adozione spontanea di misure migliorative (*i.e.* ampliamento accessi consentiti, assistenza alla clientela, eliminazione del blocco, possibilità di revocare il consenso prestato, etc.).

VI. PARERE DELL'AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI

66. Poiché la pratica commerciale oggetto del presente provvedimento è stata diffusa anche tramite *App* a mezzo *internet*, in data 13 marzo 2025 è stato richiesto il parere all'AGCOM, ai sensi dell'articolo 27, comma 6, del Codice del consumo.

67. Con comunicazione pervenuta in data 15 aprile 2025[95], la suddetta Autorità ha espresso il proprio parere rilevando che la pratica in esame, sulla base della documentazione istruttoria, si riferisce alle comunicazioni e alle attività attuate dalla Società tramite *Internet* che costituisce una rete di comunicazione globale, in grado di offrire velocemente all'utente una vasta sequenza di

---

91 Cfr. PS12604 - *Mooney - Carta con Iban.*

92 Doc. 66, cit., pag. 23.

93 Poste richiama sul punto alcuni precedenti giurisprudenziali tra cui: Consiglio di Stato, Sez. VI, sentenza n. 4359/2019; Corte di Cassazione, Sez. 3 Civ., sentenza n. 3780/2024.

94 Doc. n. 66, cit., pag. 28.

95 Doc. n. 77 (Parere AGCOM prot. 0028336 del 15/04/2025)

informazioni atte ad influenzarne il comportamento. Pertanto, "*con riferimento al caso di specie, il mezzo di comunicazione e acquisto utilizzato, in relazione al servizio offerto dalla Società, risulta idoneo a sviluppare un significativo impatto sui consumatori che, sulla base delle informazioni lette nei siti/App utilizzati dalla Società, potrebbero essere indotti ad assumere una decisione commerciale che altrimenti non avrebbero preso, così sviluppando in concreto la piena potenzialità delle modalità di promozione e vendita utilizzate*". L'AGCOM ha ritenuto, quindi, che nel caso di specie, "Internet *sia uno strumento di comunicazione idoneo a influenzare significativamente la realizzazione della pratica commerciale rispetto alla quale è richiesto il parere* […]".

VII. IL PARERE DELL'AUTORITÀ DI REGOLAZIONE

68. Poiché la pratica commerciale oggetto del presente provvedimento riguarda il settore dei servizi di pagamento, in data 13 marzo 2025 è stato richiesto il parere alla Banca d'Italia, ai sensi e per gli effetti di cui all'articolo 27, comma 1-*bis*, del Codice del consumo. Il parere è pervenuto in data 2 aprile 2025[96] e reca, in sintesi, le osservazioni e valutazioni che seguono.

69. Banca d'Italia, sulla base della documentazione istruttoria, ha espresso il proprio parere, osservando che, per i profili di propria competenza, "*l'implementazione del sistema* anti-malware *è coerente con il quadro normativo in tema di prevenzione delle frodi ed è in linea con le aspettative di questo Istituto circa l'esigenza di garantire un utilizzo sicuro degli strumenti di pagamento e una piena tutela della clientela, specie in un contesto di mercato connotato da fenomeni fraudolenti in crescita; ciò, considerato anche che è stato in ogni caso assicurato ai clienti che hanno negato l'accesso ai dati la continuità nei servizi di pagamento*".

VIII. IL PARERE DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

70. In data 13 marzo 2025, in considerazione dei potenziali impatti della condotta oggetto del procedimento in materia di protezione dei dati personali, è stato richiesto il parere al Garante per la Protezione dei dati personali. Il parere è pervenuto in data 14 aprile 2025[97] e reca, in sintesi, le osservazioni e valutazioni che seguono.

71. *[Omissis]*.

72. *[Omissis]*.

IX. VALUTAZIONI

Premessa

73. Il procedimento in esame ha accertato l'esistenza di una pratica commerciale scorretta posta in essere dalla società Poste Italiane S.p.A. nell'offerta dei servizi di pagamento e consistente nel blocco (o nella prospettazione di blocco) dell'utilizzo delle *App* Banco Posta e PostePay - installate negli *smartphone* con sistema operativo Android.

74. Tale pratica si configura come aggressiva in violazione degli articoli 24 e 25 del Codice del consumo, in quanto la possibilità per i clienti di Poste di poter continuare ad avvalersi delle predette *App* è stata subordinata al rilascio obbligatorio del consenso all'accesso a una pluralità di dati

[96] Doc. n. 73 (Parere Banca d'Italia - prot. 0024219 del 02/04/2025).

[97] Doc. n. 76 (Parere GPDP - prot. 0027999 del 14/04/2025).

presenti nel proprio *smartphone*, in base a una richiesta genericamente motivata dalla necessità di garantire la sicurezza da eventuali frodi agli utenti delle *App* Banco Posta e PostePay.

75. La pratica è, altresì, risultata in contrasto con il dovere di diligenza professionale prescritto all'articolo 20 del Codice del consumo in considerazione dell'asimmetria informativa che caratterizza i rapporti tra intermediari finanziari con i propri clienti, che, nel caso di specie, deve ritenersi particolarmente elevato in considerazione dell'importanza del Professionista e delle caratteristiche della sua clientela che, *[omissis]*.[98], ricomprende soggetti non particolarmente esperti e informati.

76. In via preliminare, occorre sgomberare il campo dal rilievo - già adombrato in corso di istruttoria ma più compiutamente sviluppato in sede di controdeduzioni al Collegio - secondo cui la condotta in esame non ricadrebbe nell'ambito di applicazione del Codice del consumo, in ragione dell'assenza di un rapporto di consumo alla stessa sotteso, imprescindibile per la configurazione di una pratica commerciale.

77. In particolare, secondo il Professionista, i dati oggetto di monitoraggio ai fini antifrode, non sarebbero configurabili come "patrimoniali" sia in ragione delle modalità di raccolta degli stessi (che avverrebbe in forma anonima mediante l'attribuzione di un codice *hash*), sia per la segregazione che, a dire del Professionista li sottrarrebbe a finalità commerciali e/o di *marketing*. Secondo Poste, pertanto, l'insussistenza di un rapporto di consumo deriverebbe dalla mancata commercializzazione dei dati dei clienti di Poste Italiane, oggetto della richiesta di autorizzazione[99].

78. Si tratta di un argomento privo di pregio atteso che, anche volendo prescindere da ogni valutazione sull'effettiva irreversibilità della natura anonima dei dati interessati[100] e sull'assenza di qualsivoglia utilizzo, anche potenziale, degli stessi per finalità commerciali, nel caso di specie il rapporto di consumo va ravvisato nella relazione contrattuale intercorrente tra il consumatore e Poste Italiane S.p.A., avente a oggetto la fornitura di servizi di pagamento anche mediante le *App* Banco Posta e PostePay.

79. Il Professionista ha, infatti, richiesto ai propri clienti di autorizzare l'accesso ai dati del proprio *smartphone* al fine di poter continuare a usufruire di una funzionalità ricompresa nel servizio da esso fornito, che costituisce parte integrante dell'offerta di Poste Italiane ai propri clienti, segnatamente la possibilità di disporre del proprio conto corrente o della propria carta di credito attraverso il canale *App*.

80. Tanto premesso, si evidenzia, altresì, che le condotte di cui trattasi, poste in essere nel periodo compreso tra aprile 2024 e febbraio 2025, hanno interessato una moltitudine di consumatori.

81. Infatti, il numero di *App* Banco Posta e PostePay[101] riconducibile ai clienti cui è stato richiesto di fornire l'autorizzazione ad accedere ai dati presenti nello *smartphone* su cui erano installate le

---

98 Doc. n. 22, cit., pag. 5.

99 Cfr. Doc. 66, cit. pagg. 16 - 18.

100 Anche se i codici *hash* sono irreversibili, gli stessi non sono perfettamente anonimi, soprattutto nel caso in cui l'*input* (un *file*, un testo o un'applicazione) è un dato che può essere facilmente indovinato o se vengono usate tecniche avanzate come le tabelle arcobaleno (*rainbow tables*) che permette di "*invertire*" l'*hash* utilizzando pre-computazioni. In pratica, queste tabelle contengono milioni di *hash* di valori comuni o frequenti (come parole comuni o password comuni). Se un *hash* corrisponde a uno di questi valori pre-calcolati, è possibile risalire al dato originale.

101 Al riguardo, il Professionista ha precisato che risulta impossibile fornire il numero degli utenti a causa della possibilità che ciascuno di essi sia dotato di più device e che il rilascio dell'autorizzazione abbia riguardato una sola delle due *App* di cui è titolare (cfr. Doc. n. 25, cit. e Doc. n. 35, cit.).

App predette per poter continuare a usufruirne, è risultato, al 30 settembre 2024, superiore ai *[10-15]* milioni[102].

82. Tutti i predetti consumatori hanno subito un pregiudizio, attuale o potenziale dalla pratica in esame, in quanto - nel periodo immediatamente successivo all'introduzione del nuovo sistema antifrode (1° maggio 2024 - 30 settembre 2024) - risulta che: ***(i)*** taluni titolari di *App* (più di *[200.000-400.000]* nel primo bimestre[103]) si sono visti bloccare l'accesso alle *stesse* per non aver concesso l'autorizzazione; ***(ii)*** altri (circa *[1.000.000-2.000.000][104])* sono stati soggetti a uno stringente limite di utilizzo delle *App*, corrispondente al numero massimo di accessi consentito in assenza di autorizzazione (tre in un primo momento e cinque successivamente); ***(iii)*** la restante parte (superiore a *[5-10]* milioni di utenti) ha assunto la scelta di consentire l'accesso ai dati presenti sui propri *smartphone,* in un contesto di condizionamento determinato dall'obbligatorietà del rilascio del consenso, pena il blocco delle *App*.

La scorrettezza della pratica

83. Poste Italiane contesta la qualificazione della pratica, sia sotto il profilo dell'omessa diligenza che della natura aggressiva della condotta.

84. In particolare, la Parte sostiene che l'aver adottato un sistema volto a tutelare i propri utenti da possibili frodi sarebbe espressione di una condotta improntata alla diligenza piuttosto che il contrario. Al riguardo, risultano del tutto inconferenti i precedenti richiamati da Poste Italiane relativi a casi in cui l'Autorità ha censurato l'inadeguatezza dei sistemi di vigilanza adottati da prestatori di servizi finanziari; ciò in quanto oggetto della contestazione in esame non è la scelta di dotarsi di un sistema antifrode, né tantomeno la valutazione dell'efficacia dello stesso rispetto ad altre possibili soluzioni.

85. Piuttosto, l'istruttoria in esame ha avuto a oggetto la scelta unilaterale di ostacolare la fruizione di una rilevante funzionalità di un servizio (*i.e.* accesso ai servizi di pagamento tramite *App*) oggetto di un rapporto contrattuale di cui consumatori interessati dalla pratica sono titolari.

86. Sul punto non può neanche trovare accoglimento l'ulteriore argomento volto a escludere l'aggressività della condotta, in quanto dal mancato accesso alle *App* non deriverebbe alcun disagio per i consumatori, essendo possibile per gli stessi fruire dei servizi Banco Posta o PostePay, sia attraverso i canali fisici che *online* (tramite *browser* accessibile anche da *smartphone o tablet*).

87. Una tale ricostruzione omette di considerare le peculiari caratteristiche di utilizzo delle *App* rispetto al canale *web* e al canale fisico che portano a escludere l'equiparabilità tra le prime e i secondi e, quindi, la loro fungibilità, dal punto di vista del consumatore.

88. In particolare, relativamente al canale *web*, giova rilevare che la struttura stessa del sistema presenti una minore facilità di utilizzo. Le *App*, infatti, differentemente dal *browser*, essendo direttamente installate sul dispositivo e integrandosi perfettamente con il sistema operativo, utilizzano interfacce più intuitive e ottimizzate che consentono un accesso più rapido ai dati e alle

---

[102] Come già precisato nella nota 54, il Professionista ha successivamente comunicato che tale dato ha subito un aumento di circa *[1-5]* milioni (Doc. n. 35, cit. pag. 3).

[103] Tale numero subisce una diminuzione nel periodo 1° maggio 2024 - 30 settembre 2024, a seguito dell'innalzamento del numero di accessi consentiti prima del blocco (da tre a cinque), disposto dal Professionista.

[104] Tale numero subisce un notevole incremento nel periodo 1° maggio 2024 - 30 settembre 2024, a seguito dell'innalzamento del numero di accessi consentiti prima del blocco (da tre a cinque), disposto dal Professionista.

funzionalità offerte. Inoltre, garantiscono una comunicazione istantanea con il consumatore, grazie al sistema di notifiche *push*, e una maggiore facilità di accesso e utilizzo, sfruttando le funzionalità del dispositivo (ad esempio, autenticazione biometrica, accesso tramite codici PIN, sensori per il riconoscimento delle impronte digitali etc.).

89. Quanto alla prospettata alternativa del canale fisico, appare di immediata evidenza la non equivalenza delle modalità di accesso (e, quindi, la fruizione del relativo servizio) per il consumatore. Recarsi presso l'Ufficio postale più vicino presenta importanti differenze dal punto di vista logistico oltre che in termini di tempo impiegato, in quanto non può escludersi che, nonostante la presenza capillare degli uffici postali sul territorio, raggiungere fisicamente lo stesso (peraltro, in orari prestabiliti) per fruire del servizio di cui si è beneficiari, possa costituire un disagio non trascurabile, anche in considerazione del fatto che alcuni utenti potrebbero trovarsi nell'impossibilità di farlo (per impedimento fisico o altra ragione).

La necessarietà della condotta

90. La condotta in esame non può ritenersi esser stata posta in essere per adempiere a un obbligo di legge o regolamentare. Nelle stesse controdeduzioni al Collegio, la Parte, diversamente da quanto sostenuto nella fase iniziale dell'istruttoria, infatti, ammette che "*l'art. 2 delle RTS richiede pertanto di implementare sistemi antifrode che tengano conto «come minimo» della presenza di segnali di* malware*, ma, per le ragioni sopraesposte, non impone (né tantomeno indica), le tecnologie o le specifiche misure tecniche di cui gli operatori devono dotarsi per ottemperare a tale obbligo*"[105].

91. In effetti, se è vero che la disciplina di cui dalla Direttiva PSD2 e i relativi *standard* tecnici RTS richiedono ai prestatori di servizi di pagamento l'adozione di processi di monitoraggio delle operazioni effettuate tramite i loro sistemi volti a intercettare i fattori di rischio - tra cui i segnali della presenza di *malware* - tali atti non giungono a indicare come deve funzionare la componente *anti malware* del sistema antifrode di cui essi devono dotarsi.

92. *[Omissis]*[106].

93. *[Omissis]*.

94. *[Omissis]*.

95. Da ultimo, non può sottacersi che i dati cui alla precedente Tabella 3, forniti dallo stesso Professionista, evidenziano che il numero di *alert*, rilevato in un arco temporale di circa sette mesi dai sistemi di controllo di Poste Italiane, è diminuito di circa tre volte per effetto dell'introduzione

---

[105] Doc. n. 66, cit., pag. 20.

[106] Articolo 6 del Regolamento (UE) 2016/679. - Liceità del trattamento.
1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per 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, in particolare se l'interessato è un minore.
La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

del nuovo sistema antifrode e che tale calo del dato degli *alert* non è riconducibile a una riduzione dei c.d. "*falsi positivi*", la cui percentuale è la medesima nei due periodi considerati. Sebbene Poste Italiane abbia precisato che i dati comunicati devono essere valutati *[omissis].*[107], dagli stessi emerge, per quel che rileva in questa sede, che all'utilizzo del nuovo sistema non è corrisposto, nei primi sette mesi di attuazione, una rilevazione maggiore o più efficiente di fenomeni fraudolenti.

La proporzionalità della condotta

96. Le risultanze istruttorie hanno, altresì, posto in rilievo che il blocco delle *App* non era l'unica soluzione possibile per tutelare i clienti di Poste da fenomeni fraudolenti.

97. La stessa Parte ha, infatti, dato conto che la quasi totalità degli operatori suoi concorrenti, per ottemperare alle prescrizioni normative antifrode, si avvale di sistemi differenti il cui funzionamento non è condizionato all'obbligatorio rilascio del consenso all'accesso dei dati in utilizzo sugli *smartphone*.

98. Ma ciò che più rileva è che in corso di procedimento il Professionista ha volontariamente provveduto a rimuovere il predetto blocco delle *App* consentendo, quindi, di continuare a utilizzarle anche ai consumatori non intenzionati a rilasciare il proprio consenso all'accesso/trattamento dei dati del proprio *smartphone,* precisando che a tali consumatori sarebbe stata, comunque, garantita adeguata tutela avverso possibili frodi, a dimostrazione dell'esistenza di una soluzione alternativa in grado di garantire il contemperamento delle esigenze di tutela antifrode con quelle di assicurare ai consumatori la piena fruizione dei servizi cui hanno aderito.

99. Peraltro, lo stesso Professionista, pur ribadendo di aver agito in buona fede nell'adozione del sistema antifrode e di non aver perseguito, tramite lo stesso, alcuna finalità commerciale, ha asserito, nel corso della seconda audizione con gli Uffici dell'11 novembre 2024, che il blocco delle *App* abbia costituito "*una misura molto impattatante*" e che, per tali ragioni "[…] *Dallo scorso settembre, quindi, il Gruppo si è attivato per cercare di trovare un'alternativa al blocco delle App, con una soluzione in grado di garantire il contemperamento delle esigenze di tutela antifrode con quelle di massima limitazione dei disagi per i consumatori derivanti dal blocco dell'App*" [108].

100. Al riguardo, Banca d'Italia, nel parere *ex* articolo 27, comma 1-*bis*, del Codice del consumo, si è espressa per la coerenza della misura adottata da Poste rispetto al quadro normativo in materia antifrode; tale circostanza. Tuttavia. non è in discussione nell'ambito del presente procedimento, per il quale non rileva affatto l'eventuale legittimità degli obiettivi perseguiti da Poste Italiane (fronteggiare i fenomeni fraudolenti), ma rilevano le modalità aggressive e contrarie alla diligenza professionale scelte per dare attuazione a siffatti obiettivi.

101. Cionondimeno, l'Autorità di regolazione, nell'affermare la funzionalità delle condotte di Poste Italiane al perseguimento del citato obiettivo, non si è pronunciata sulla proporzionalità delle stesse rispetto alla finalità perseguita, limitandosi a osservare che ai clienti che hanno negato l'accesso ai dati è stata comunque assicurata "*la continuità nei servizi di pagamento*", tramite gli altri canali a loro disposizione (*browser* e sportelli fisici).

102. A tale ultimo proposito, si osserva che l'esistenza di canali alternativi che, nel periodo oggetto di istruttoria, hanno garantito ai clienti di Poste Italiane di poter effettuare pagamenti e gestire e

[107] Doc. n. 40, pag. 4, cit..

[108] Doc. n. 40, cit., pag. 1.

monitorare i propri risparmi, assume specifico rilievo per la disciplina di competenza di Banca d'Italia (che, infatti, vi ha fatto espressamente riferimento "*per i profili di competenza della Banca d'Italia*") la quale prevede, quale condizione di operatività dei prestatori di servizi di pagamento, l'obbligo di garantire la continuità di tali servizi, con l'obiettivo di scongiurarne il rischio di interruzione, vale a dire la preclusione di accedere con qualsivoglia modalità ai servizi di pagamento[109].

103. La tutela apportata dal Codice del consumo, di cui il presente provvedimento accerta il mancato soddisfacimento, attiene, invece, al diritto dei consumatori di poter fruire di tutte le prerogative previste dall'offerta alla quale hanno aderito, che nel caso di specie comprendeva anche l'accesso ai servizi di Banco Posta e PostePay tramite *App*.

104. Ciò anche in considerazione del fatto che, come rilevato, per le finalità di cui alla disciplina sulle pratiche commerciali scorrette, le alternative a disposizione (accesso via *browser* e via canali fisici) non appaiono equiparabili e, quindi, sostituibili per il consumatore.

Conclusioni

105. Alla luce degli elementi suesposti, la condotta posta in essere da Poste Italiane descritta al punto II della presente comunicazione integra una pratica commerciale scorretta in violazione degli articoli 20, 24 e 25 del Codice del consumo, in quanto contraria alla diligenza professionale e idonea condizionare indebitamente e in misura apprezzabile il comportamento economico dei consumatori.

X. QUANTIFICAZIONE DELLA SANZIONE

106. Ai sensi dell'articolo 27, comma 9, del Codice del consumo, con il provvedimento che vieta la pratica commerciale scorretta, l'Autorità dispone l'applicazione di una sanzione amministrativa pecuniaria da 5.000 a 10.000.000 euro, tenuto conto della gravità e della durata della violazione.

107. In ordine alla quantificazione della sanzione deve tenersi conto, in quanto applicabili, dei criteri individuati dall'articolo. 11 della legge n. 689/1981, in virtù del richiamo previsto all'articolo 27, comma 13, del Codice del consumo: in particolare, della gravità della violazione, dell'opera svolta dall'impresa per eliminare o attenuare l'infrazione, della personalità dell'agente, nonché delle condizioni economiche dell'impresa stessa.

108. Rispetto alla gravità della violazione, si tiene conto, nella fattispecie in esame, delle caratteristiche del settore dei servizi finanziari e di pagamento in cui la pratica è stata posta in essere, il quale risulta caratterizzato da un grado molto elevato di asimmetria informativa tra Professionista e consumatori, che rende particolarmente rigoroso il livello di diligenza richiesto, soprattutto da parte di operatori aventi la rilevanza e dimensione di Poste Italiane, anche tenuto conto delle caratteristiche della sua clientela, che ricomprende soggetti non particolarmente esperti e informati.

109. Rileva, inoltre, che la pratica in esame presenta profili di aggressività, consistenti nell'indebito condizionamento degli utenti delle *App* Banco Posta e PostePay di *smartphone* con sistema operativo Android cui è stato prospettato, ovvero concretamente applicato, il diniego all'accesso alle *App* relative alla gestione dei propri pagamenti e risparmi; che la stessa appare di ampia diffusione, nella misura in cui ha interessato diversi milioni di clienti e che è stata realizzata da uno dei principali operatori del settore dei servizi finanziari e di pagamento.

---

[109] Cfr., tra gli altri, articolo 5, par. 1, Direttiva PSD2.

Con riguardo alla dimensione economica, rileva che Poste Italiane è a capo di un Gruppo di notevoli dimensioni e che, dal bilancio di esercizio consolidato al 31 dicembre 2023, ha realizzato ricavi pari a 11.989 milioni di euro, con un EBITDA pari a 3.431 milioni di euro[110].

110. Per quanto riguarda poi la durata della violazione, dagli elementi disponibili in atti la pratica commerciale descritta al punto II risulta posta in essere da Poste Italiane a partire dal mese di aprile 2024 e almeno fino al 18 febbraio 2025, data a partire dalla quale il Professionista ha comunicato di aver rimosso il blocco delle *App*[111], nonché garantito la possibilità di rivalutare la scelta di autorizzare l'accesso ai dati presenti sul proprio dispositivo da parte dei clienti che l'avevano accordata.

111. Sussiste, nel caso di specie, la circostanza attenuante del ravvedimento operoso, in quanto la Società ha dato conto di aver adottato, a far data dal 18 febbraio 2025, una serie di misure correttive e ripristinatorie, prevedendo interventi a tutela dei consumatori interessati dal blocco e consentendo di confermare/revocare la propria scelta anche a coloro che avevano già fornito il consenso all'accesso ai propri dati.

Sulla base di tali elementi, tenuto conto che il fatturato registrato dal Professionista è di decine di miliardi di euro, si ritiene di fissare l'importo della sanzione amministrativa pecuniaria applicabile nella misura di 6.000.000 € (seimilioni di euro), che vengono ridotti a 4.000.000 € (quattromilioni di euro), in considerazione della sussistenza della predetta circostanza attenuante.

RITENUTO, pertanto, tenuto conto dei pareri di Banca d'Italia, dell'Autorità per le Garanzie nelle Comunicazioni e del Garante per la protezione dei dati personali, sulla base delle considerazioni suesposte, che la pratica commerciale in esame, posta in essere dalla società Poste Italiane S.p.A., risulta scorretta ai sensi degli articoli 20, 24 e 25 del Codice del consumo in quanto contraria alla diligenza professionale e idonea a falsare in misura apprezzabile il comportamento economico del consumatore medio in relazione alle proprie scelte di consumo nel settore dei servizi di pagamento;

DELIBERA

a) che la pratica commerciale descritta al punto II del presente provvedimento, posta in essere dalle società Poste Italiane S.p.A., costituisce, per le ragioni e nei limiti esposti in motivazione, una pratica commerciale scorretta ai sensi degli articoli 20, 24 e 25 del Codice del consumo;

b) di irrogare alla società Poste Italiane S.p.A. una sanzione amministrativa pecuniaria di 4.000.000 € (quattromilioni di euro).

La sanzione amministrativa irrogata deve essere pagata entro il termine di trenta giorni dalla notificazione del presente provvedimento, utilizzando i codici tributo indicati nell'allegato modello F24 con elementi identificativi, di cui al Decreto Legislativo n. 241/1997.

Il pagamento deve essere effettuato telematicamente con addebito sul proprio conto corrente bancario o postale, attraverso i servizi di *home-banking* e CBI messi a disposizione dalle banche o da Poste Italiane S.p.A., ovvero utilizzando i servizi telematici dell'Agenzia delle Entrate, disponibili sul sito *internet www.agenziaentrate.gov.it*.

---

110 Cfr. "*Relazione Finanziaria Annuale 2023*", in https://www.posteitaliane.it/it/bilanci-e-relazioni.html#/.

111 Doc. 61, cit..

Decorso il predetto termine, per il periodo di ritardo inferiore a un semestre, devono essere corrisposti gli interessi di mora nella misura del tasso legale a decorrere dal giorno successivo alla scadenza del termine del pagamento e sino alla data del pagamento. In caso di ulteriore ritardo nell'adempimento, ai sensi dell'articolo 27, comma 6, della legge n. 689/1981, la somma dovuta per la sanzione irrogata è maggiorata di un decimo per ogni semestre a decorrere dal giorno successivo alla scadenza del termine del pagamento e sino a quello in cui il ruolo è trasmesso al concessionario per la riscossione; in tal caso la maggiorazione assorbe gli interessi di mora maturati nel medesimo periodo.
Dell'avvenuto pagamento deve essere data immediata comunicazione all'Autorità attraverso l'invio della documentazione attestante il versamento effettuato.

Il presente provvedimento sarà notificato ai soggetti interessati e pubblicato nel Bollettino dell'Autorità Garante della Concorrenza e del Mercato.

Ai sensi dell'articolo 27, comma 12, del Codice del consumo, in caso di inottemperanza al provvedimento, l'Autorità applica la sanzione amministrativa pecuniaria da 10.000 a 10.000.000 euro. Nei casi di reiterata inottemperanza, l'Autorità può disporre la sospensione dell'attività di impresa per un periodo non superiore a trenta giorni.

Avverso il presente provvedimento può essere presentato ricorso al TAR del Lazio, ai sensi dell'articolo 135, comma 1, lettera b), del Codice del processo amministrativo (Decreto legislativo 2 luglio 2010, n. 104), entro sessanta giorni dalla data di notificazione del provvedimento stesso, fatti salvi i maggiori termini di cui all'articolo 41, comma 5, del Codice del processo amministrativo, ovvero può essere proposto ricorso straordinario al Presidente della Repubblica ai sensi dell'articolo 8 del Decreto del presidente della Repubblica 24 novembre 1971, n. 1199 entro il termine di centoventi giorni dalla data di notificazione del provvedimento stesso.

IL VICE SEGRETARIO GENERALE
Serena Stella

IL PRESIDENTE
Roberto Rustichelli