GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Provvedimento del 13 novembre 2026 [10321455]

VEDI ANCHE Comunicato stampa del 14 novembre 2026

[doc. web n. 10321455]

- ENGLISH VERSION

Provvedimento del 13 novembre 2026

Registro dei provvvedimenti
n. 815 del 13 novembre 2026

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

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

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196), (di seguito "Codice");

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

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, adottato con deliberazione del 28 giugno 2000 (doc. web n. 1098801);

RELATORE il prof. Pasquale Stanzione;

1. FATTO E SVOLGIMENTO DELL'ISTRUTTORIA

1.1. Origine dell'istruttoria preliminare

Il presente procedimento trae origine da una segnalazione presentata il 10 luglio 2025 dal Centro Tutela Consumatori Utenti di Bolzano (Verbraucherzentrale Südtirol, di seguito "CTCU") nei confronti della società di diritto irlandese Meta Platforms Ireland Ltd (da qui in avanti "Meta" o "la Società" o "il titolare").

La segnalazione del CTCU. In base alla segnalazione, Meta, senza preavviso, avrebbe apportato una delicata modifica all'applicazione Facebook in uso negli smartphone dei propri utenti, e, conseguentemente, al rapporto in essere con i medesimi, introducendo una funzionalità denominata "*Suggerimenti personalizzati da condividere provenienti dalla galleria*", articolata in due sotto-opzioni: una, mediante la quale Meta accederebbe ai metadati e ai contenuti della galleria fotografica del dispositivo (video preferiti, *timestamp* degli scatti) per generare automaticamente contenuti già editati (transizioni, musica, effetti); l'altra, che interverrebbe mentre l'utente naviga su Facebook, mostrando immagini dalla propria galleria locale come suggerimenti per possibili pubblicazioni sul social network. Il CTCU ha sostenuto che gli utenti non sarebbero stati informati della modifica né avrebbero espresso un valido consenso, trattandosi di un'opzione con consenso "tacitamente preimpostato", e ha prospettato un collegamento con l'addestramento dei sistemi di intelligenza artificiale di Meta.

L'oggetto del provvedimento. Il presente provvedimento ha ad oggetto la funzionalità "Ottieni suggerimenti dalla galleria quando navighi su Facebook" (di seguito, la "Funzionalità"), accessibile dalla pagina delle impostazioni "Suggerimenti da condividere provenienti dalla galleria". Non è oggetto del procedimento l'opzione "Suggerimenti personalizzati da condividere provenienti dalla galleria", che Meta ha dichiarato non essere mai stata disponibile nella Regione europea e visibile ad alcuni utenti per un errore di visualizzazione (c.d. bug), né la distinta funzionalità "Ottieni idee creative su misura per te consentendo l'elaborazione nel cloud della galleria fotografica", che Meta riferisce essere stata lanciata nell'Unione europea all'inizio del 2026 e che la Comunicazione di avvio non ha considerato. Non è oggetto di accertamento, per l'assenza di elementi, l'eventuale impiego dei contenuti non pubblicati per l'addestramento dei sistemi di intelligenza artificiale, che Meta ha negato di effettuare.

Sotto un profilo di sistematica espositiva, si rappresenta la necessità di illustrare preliminarmente le caratteristiche della Funzionalità della App Facebook inserita nella pagina delle impostazioni denominata "Suggerimenti da condividere provenienti dalla galleria".

1.2. Caratteristiche principali della Funzionalità

La Funzionalità consente a Meta di presentare all'utente, durante la navigazione sulla piattaforma Facebook, suggerimenti di condivisione di base provenienti dalla galleria del proprio dispositivo.

Perché sia operativa la Funzionalità è necessario che l'opzione "*Ottieni suggerimenti dalla galleria quando navighi su Facebook*" - presente nelle impostazioni della App Facebook - sia impostata su "attiva", come confermato anche da Meta ("*Quando un utente concede l'autorizzazione del dispositivo per la propria galleria, l'opzione di attivazione illustrata nella* ***Figura 1*** *per ricevere suggerimenti di condivisione di base viene impostata su "attivo"* (per chiarezza espositiva si riporta di seguito anche la richiamata Figura 1).



La Società ha precisato che gli utenti possono esercitare il controllo sulla Funzionalità in qualsiasi momento agendo sull'apposito tasto posto in corrispondenza dell'indicazione "*Ottieni suggerimenti dalla galleria quando navighi su Facebook*".

1.3. Attività svolta

Richiesta di informazioni. Con nota del 27 ottobre 2025 (prot. n. 142506), formulata nell'esercizio della competenze riconducibili all'art. 122 del Codice, l'Ufficio ha chiesto a Meta informazioni e documenti sulla Funzionalità: le modalità con cui gli utenti italiani sono stati informati prima dell'attivazione; il funzionamento tecnico e il perimetro del trattamento; la base giuridica; l'interfaccia e il meccanismo di acquisizione del consenso, specificando se l'impostazione predefinita fosse "attiva" o "inattiva"; gli eventuali

utilizzi ulteriori, anche per l'addestramento di modelli di intelligenza artificiale; i tempi di conservazione; le misure sulle categorie particolari di dati e sulle immagini di minori; le procedure di revoca.

Riscontro Meta. In riscontro alla richiesta di informazioni dell'Ufficio, in primo luogo Meta ha contestato formalmente la competenza del Garante ad agire direttamente, sostenendo che il trattamento in questione ricade sotto la giurisdizione esclusiva della *Data Protection Commission* irlandese (di seguito, "DPC"), in quanto autorità capofila, ai sensi del meccanismo dello sportello unico (*One-Stop-Shop*) previsto dall'art. 56 del Regolamento. Inoltre, Meta ha ritenuto infondata la tesi del Garante secondo cui la Funzionalità rientrerebbe nell'ambito della direttiva e-Privacy (e quindi dell'art. 122 del Codice) in assenza di "strumenti di tracciamento".

Le dichiarazioni di Meta. Meta ha affermato che la Funzionalità è disponibile dal 2023 e non sarebbe collegata all'intelligenza artificiale generativa, contestando preliminarmente la competenza del Garante, in favore della DPC, nonché l'applicabilità dell'art. 122 del Codice, in assenza di "strumenti di tracciamento". Pur dichiarando di fornire le informazioni "volontariamente", Meta ha rappresentato, in sintesi, che: (i) l'accesso alla galleria richiede un'autorizzazione a livello di sistema operativo, che l'utente può concedere in forma completa o limitata ai contenuti selezionati; (ii) la Funzionalità tratta le foto più recenti e i "metadati di base" (data e ora dello scatto, foto contrassegnate come preferite, tipologia o orientamento della foto), mentre non è menzionato l'uso di dati di geolocalizzazione o di dati EXIF completi; (iii) quando l'utente concede l'autorizzazione del dispositivo, l'opzione "Ottieni suggerimenti dalla galleria quando navighi su Facebook" è impostata su "attivo", mentre per gli altri utenti è "inattiva" per impostazione predefinita; (iv) quando la Funzionalità è *attiva* "*Meta presenta all'utente, durante la navigazione su Facebook, suggerimenti di condivisione di base provenienti dalla sua galleria*"; (v) la base giuridica è la necessità contrattuale per gli utenti con piena capacità giuridica e il legittimo interesse per i minorenni; (vi) il trattamento avverrebbe interamente sul dispositivo e non determinerebbe il trattamento di categorie particolari di dati; (vii) la trasparenza sarebbe garantita dall'informativa sulla privacy e dalle informazioni fornite nel prodotto. Meta ha altresì dichiarato di aver trasmesso copia della risposta alla DPC "a titolo di cortesia".

Accertamento tecnico. Sulla base delle dichiarazioni rese da Meta, l'Ufficio ha richiesto al Dipartimento Tecnologie Digitali e Sicurezza Informatica del Garante, con nota interna del 2 dicembre 2025 (prot. n. 168848), una valutazione di carattere tecnico sulla Funzionalità, finalizzata a descriverne le principali caratteristiche con riguardo al consenso dell'utente e al trattamento dei dati personali, nonché sull'ambito di applicazione dell'art. 5, par. 3, della direttiva 2002/58/CE ("direttiva ePrivacy").

Le risultanze della Relazione tecnica. L'analisi tecnica, resa con nota prot. n. 76045 del 18 maggio 2026 (di seguito, la "Relazione tecnica"), è stata condotta attraverso l'installazione *ex novo* dell'App Facebook su uno smartphone Android dotato del sistema operativo Android 14, consentendo di osservare il comportamento della app in condizioni di primo utilizzo, e si è avvalsa di strumenti tecnici quali l'app "Apk Analyzer" e l'ambiente di sviluppo Android Studio per l'analisi del file AndroidManifest.xml (file di configurazione che dichiara al sistema operativo, cosa l'app è e cosa intende fare) estratto dal pacchetto APK della versione 548.1.0.51.64 dell'applicazione, prelevato da un sito di terze parti e verificato nell'autenticità mediante lo strumento apksigner. Ne sono emersi i seguenti elementi:

- al primo avvio l'accesso a "Foto e video" risulta negato; l'app può accedervi solo dopo che l'utente abbia accordato le autorizzazioni di sistema operativo, mediante un'unica richiesta riferita sia alle foto sia ai video, benché si tratti di due distinte autorizzazioni (READ_MEDIA_IMAGES e READ_MEDIA_VIDEO);

- la voce "Ottieni suggerimenti dalla galleria quando navighi su Facebook" risulta preimpostata come attiva, ma, in assenza dell'autorizzazione di sistema operativo, non propone alcun suggerimento: la Funzionalità non può operare finché l'utente non concede le autorizzazioni;

- al primo tentativo di creare un post con una sola foto, una storia o un reel, l'app presenta una schermata secondo cui l'accesso alla galleria serve a "condividere foto e video, ricevere suggerimenti sulle foto da caricare e abilitare altre funzioni", e incanala l'utente verso la concessione delle autorizzazioni ampie READ_MEDIA; l'accesso concesso è, di regola, permanente e può essere revocato solo nelle impostazioni del dispositivo;

- la versione Android 13 è stata introdotta nel giugno 2022 e, a livello di sistema, prevedeva *permission* per l'accesso a foto e video da parte delle diverse App secondo le due opzioni "Consenti tutto" e "Non consentire"; l'opzione "Consenti accesso limitato" è stata un'innovazione di Android 14, introdotta invece nell'autunno 2023;

- il file Manifest dell'App Facebook dichiara le autorizzazioni READ_MEDIA_IMAGES, READ_MEDIA_VIDEO, READ_MEDIA_VISUAL_USER_SELECTED e ACCESS_MEDIA_LOCATION (relativa ai metadati EXIF di localizzazione): se concesse con un'unica finestra di sistema, l'autorizzazione sulle foto comprende anche quella sui dati di ubicazione, senza una seconda richiesta; la Relazione tecnica rileva che è "molto probabile" che l'app si avvalga di tale modalità, pur non potendo verificarlo;

- le autorizzazioni READ_MEDIA, se concesse con l'opzione "Consenti tutto", abilitano l'app a leggere tutte le foto e i video, ad effettuarne qualunque elaborazione, localmente o in cloud, e, se l'app dispone anche dell'autorizzazione INTERNET (concessa a quasi tutte le app all'installazione), a trasmetterli ai sistemi del fornitore; se l'utente utilizzava già l'app al momento dell'aggiornamento ad Android 13 e questa disponeva della precedente autorizzazione READ_EXTERNAL_STORAGE, al momento dell'introduzione della Funzionalità le autorizzazioni READ_MEDIA risultavano concesse automaticamente;

- per la pubblicazione di una singola foto, Android mette a disposizione dal 2023 il meccanismo del "photo picker", che consente alle app di accedere alle sole foto selezionate in quel momento senza richiedere autorizzazioni di sistema; la Funzionalità, invece, richiede per sua natura un accesso più ampio e continuativo, ma avrebbe dovuto essere oggetto di una richiesta separata, collegata solo ad essa e disattivata per impostazione predefinita; Meta ha invece fuso in un'unica richiesta più funzionalità con requisiti di accesso diversi;

- l'app Facebook è un software proprietario, il cui codice non è disponibile, e il traffico verso i sistemi di Meta è cifrato: l'Autorità non è in grado di verificare analiticamente quali dati siano trasmessi, né di escludere che l'app trasmetta le foto e i relativi metadati ai sistemi di Meta senza che l'utente ne abbia contezza; un'analisi black box del traffico sarebbe lunga, onerosa e dall'esito incerto.

La Relazione tecnica ha concluso che quanto rilevato ricade nell'ambito di applicazione dell'art. 5, par. 3 della direttiva ePrivacy, nella misura in cui l'accesso ai dati avviene attraverso meccanismi informatici (es. le API del sistema operativo Android) e consentono a Meta di accedere alle informazioni memorizzate nel dispositivo terminale ("*gaining access to information already stored in the terminal equipment*").

2. AVVIO DEL PROCEDIMENTO PER L'ADOZIONE DEI PROVVEDIMENTI CORRETTIVI E SANZIONATORI E DIFESE DELLA PARTE

2.1. Avvio del procedimento (art. 166, comma 5, del Codice)

L'atto di avvio del procedimento. In base all'esame degli elementi acquisiti nel corso delle attività sopra descritte e all'accertamento delle presunte violazioni, con nota del 29 luglio 2026 (prot. n. 115205), notificata ai sensi dell'art. 166, comma 5, del Codice, l'Ufficio ha avviato il procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento nei confronti del titolare del trattamento, invitando lo stesso a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall'Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, della l. 24 novembre 1981, n. 689).

Le violazioni contestate e il perimetro della contestazione. Le presunte violazioni contestate sono relative all'art. 122, commi 1 e 2, del Codice, anche in relazione agli artt. 6, 7, 12 e 13 del regolamento (UE) 2016/679, per aver effettuato accessi ad informazioni archiviate nei dispositivi mobili degli utenti, segnatamente immagini fotografiche, video e relativi metadati, in assenza del consenso, o di altra valida base di legittimità, e senza aver informato gli utenti stessi secondo metodologie che assicurino la loro effettiva consapevolezza.

Il perimetro della violazione è circoscritto a tutti gli utenti italiani che hanno installato l'app Facebook nel proprio device dotato di sistema operativo Android.

Accesso agli atti e proroga del termine difensivo. Con nota del 5 agosto 2026 (protocollata il 6 e il 7 agosto 2026, prott. nn. 119078 e 119465) Meta ha chiesto l'accesso agli atti e una proroga di quarantacinque giorni del termine per le difese. Con nota del 10 agosto 2026 (prot. n. 119976) l'Ufficio ha trasmesso l'unico atto non ancora nella disponibilità della Società (la nota interna del 2 dicembre 2025 con tre allegati) e ha concesso la proroga, fissando il termine al 12 ottobre 2026. Con nota del 14 settembre 2026 (prot. n. 131503) Meta ha segnalato che la ricezione degli allegati era stata impedita dai propri sistemi di sicurezza, perché trasmessi in formato compresso ".7z" non accettato dai propri server e che la comunicazione del 10 agosto era stata inviata a un indirizzo errato di uno dei propri difensori; ha chiesto il reinvio e ha eletto domicilio presso i propri avvocati italiani. L'Ufficio ha ritrasmesso la documentazione in formato pdf, all'indirizzo corretto, il 16 settembre 2026 (prot. n. 132333).

2.2. Difese della Parte (art. 166, comma 6, del Codice)

La memoria difensiva di Meta. Con memoria del 12 ottobre 2026, trasmessa a mezzo posta elettronica e PEC e protocollata il 13 ottobre 2026 (prot. n. 145274), Meta ha chiesto l'archiviazione del procedimento o il non luogo a provvedere, senza formulare richiesta di audizione. Ha prodotto la procura speciale (all. A), le schermate dell'impostazione della Funzionalità (doc. 1), dell'avviso che precede la richiesta di autorizzazione (doc. 2), dei passaggi autorizzativi del sistema operativo (doc. 3), della pagina di impostazioni aggiornata (doc. 4) e il bilancio d'esercizio al 31 dicembre 2024 di Meta Platforms Ireland Limited (doc. 5). Le difese possono essere così sintetizzate:

- in via preliminare, la contestazione sarebbe formulata in termini generici, priva di raccordo tra le disposizioni del Regolamento elencate al par. 6 dell'atto di avvio e le osservazioni svolte nel corpo dell'atto, con grave pregiudizio per il diritto di difesa;

- in via principale, l'art. 122 del Codice e l'art. 5, par. 3, della direttiva ePrivacy non troverebbero applicazione, perché richiederebbero l'impiego di una rete di comunicazione elettronica e l'uscita delle informazioni dal dispositivo, secondo la lettura che la Società ricava dalle Linee guida EDPB 2/2023 (par. 32, 44 e 53). La Funzionalità opererebbe interamente sul dispositivo (on-device), leggendo soltanto metadati di base (data e ora) e senza trasmettere alcun dato ai server di Meta, e il trattamento si esaurirebbe nel suggerimento rivolto all'utente. Il Garante si fonderebbe così su una capacità meramente teorica delle autorizzazioni READ_MEDIA e non su un accesso effettivo. Meta qualifica inoltre l'app come "*servizio basato su software*" e non come rete di comunicazione elettronica, e presenta la pubblicazione del contenuto suggerito come una "Fase di Pubblicazione" distinta, avviata dall'utente e sottratta, a suo dire, alla contestazione;

- sul piano della competenza, le contestazioni relative agli artt. 6, 7, 12 e 13 del Regolamento ricadrebbero nella competenza esclusiva della DPC, quale autorità capofila (art. 56 del Regolamento), non ricorrendo alcuna eccezione allo sportello unico (Corte di giustizia, sentenza del 15 giugno 2021, C-645/19, Facebook Belgium, punto 74; EDPB, parere 5/2019 del 12 marzo 2019 sull'interazione tra la direttiva e-privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati), e l'art. 122 del Codice, quale *lex specialis*, non potrebbe ampliare la competenza del Garante. La Società riconosce tuttavia che la direttiva ePrivacy non prevede alcun meccanismo di sportello unico e che il Garante è competente a far rispettare le norme nazionali di recepimento, ove applicabili (memoria, §4.1);

- in ogni caso, l'autorizzazione di sistema operativo costituirebbe un'azione positiva dell'utente e, quindi, un consenso libero, specifico, informato e inequivocabile, riferito a un'unica finalità (facilitare la condivisione dei contenuti) e revocabile in qualsiasi momento; un unico consenso potrebbe coprire più trattamenti con la medesima finalità (considerando 32 del Regolamento; Linee guida EDPB 5/2020). Il controllo in-app ("Toggle della Funzionalità in-App") non sarebbe un meccanismo di consenso (memoria, §4.31) e non equivarrebbe a una casella preselezionata (Corte di giustizia, sentenze del 1° ottobre 2019, C-673/17, Planet49, e dell'11 novembre 2020, C-61/19, Orange România). Meta ammette tuttavia che in passato il controllo poteva apparire "attivo" prima che l'utente concedesse l'autorizzazione di sistema, contrariamente a quanto dichiarato nella risposta del 14 novembre 2025, e riferisce di avervi posto rimedio con la versione 581 dell'app, precisando che gli utenti non aggiornati continuano a visualizzare l'interfaccia precedente (memoria, §4.33 e nota 7).

Ammette altresì che l'autorizzazione si applica "*all'App nel suo complesso*" e che la Funzionalità "*non può operare su una base 'una foto alla volta'*" (memoria, §5.35 e §6.2);

− in ulteriore subordine, l'accesso sarebbe strettamente necessario per un servizio esplicitamente richiesto dall'utente, e cioè il "*processo efficiente ed efficace di caricamento delle fotografie*" (memoria, §4.37), tesi svolta in un solo paragrafo e priva di elementi a supporto. Quanto al "photo picker", Meta osserva che il suggerimento non corrisponderebbe ad alcuna contestazione e sarebbe comunque errato, perché la Funzionalità non potrebbe operare "una foto alla volta" e il modello di autorizzazioni di Android non consentirebbe richieste per singola funzionalità (memoria, §6.1-6.3);

− Meta precisa di non fondare il trattamento sul consenso quale base giuridica ai sensi del Regolamento, ma sulla necessità contrattuale (utenti con piena capacità) e sul legittimo interesse (utenti con capacità limitata, §5.23), basi distinte dai requisiti dell'art. 122 del Codice, e ritiene non pertinente il richiamo all'art. 7 del Regolamento; per l'accesso farebbe valere il solo consenso espresso con l'autorizzazione di sistema e, in subordine, la stretta necessità. Quanto all'informazione, gli utenti sarebbero informati dall'informativa generale sulla privacy (che dal luglio 2022 farebbe riferimento ai metadati delle foto), dall'avviso che precede la richiesta di autorizzazione, dal suggerimento di condivisione stesso e dall'articolo del Centro Assistenza pubblicato nell'aprile 2026 (§5.32); non sarebbe richiesta "*una notifica aggiuntiva e separata*" (§5.31), trattandosi di dati "non sensibili" e di un trattamento "*coerente con le funzionalità principali dell'App*" (§5.30). Non sussisterebbero modelli di progettazione ingannevoli, la denominazione della Funzionalità non sarebbe fuorviante e l'autorizzazione ACCESS_MEDIA_LOCATION, dichiarata nel Manifest a livello di applicazione, non sarebbe utilizzata dalla Funzionalità (§5.34-5.36);

− in via di estremo subordine, non vi sarebbe alcun danno e la violazione sarebbe di minima gravità, perché i dati sarebbero soltanto metadati di base non sensibili; la stima di circa 20 milioni di utenti indicata dall'Autorità sarebbe priva di supporto e non corretta, senza che la Società indichi alcuna cifra alternativa; potrebbe al più essere adottato un richiamo non pubblico.

3. VALUTAZIONI DELL'AUTORITÀ

3.1 Quadro normativo e premessa metodologica

Le posizioni espresse da Meta sia in sede di riscontro alla richiesta di informazioni che con la memoria difensiva non sono idonee ad escludere la responsabilità di Meta in ordine alla contestazione mossa e, inoltre, impongono all'Autorità di formulare delle necessarie precisazioni preliminari in ordine al metodo con cui la vicenda in argomento è stata affrontata.

Il parametro della valutazione. La contestazione ha ad oggetto la violazione dell'art. 122 del Codice. È tale disposizione, e non il Regolamento né il quadro interpretativo europeo richiamato da Meta, il parametro con cui l'Autorità valuta la condotta: l'art. 122 definisce la condotta vietata (l'accesso a informazioni già archiviate nel terminale dell'utente in assenza del suo consenso, previa informazione) ed è la norma la cui violazione è sanzionata ai sensi dell'art. 166, comma 2, del Codice. Le difese di Meta spostano invece il confronto su un terreno diverso: quello dell'ambito tecnico dell'art. 5, par. 3, della direttiva ePrivacy, quale ricostruito dagli Orientamenti 2/2023 dell'EDPB, e quello delle disposizioni del Regolamento. L'Autorità non intende sottrarsi al confronto su tali profili, che affronta nel merito nei paragrafi seguenti. Ritiene tuttavia necessario ribadire che l'elemento normativo in base al quale l'Autorità procede è l'art. 122 del Codice, interpretato in modo conforme alla direttiva che esso recepisce, e che le osservazioni della Società e le Linee guida richiamate rilevano nei limiti in cui contribuiscono a chiarire la portata di tale disposizione, non nel senso di sostituirne il testo, né di restringerne l'ambito di applicazione.

In questa prospettiva l'analisi è articolata sugli elementi dell'art. 122: l'accesso a informazioni archiviate nel terminale (par. 3.3), il consenso e l'informazione dell'utente (parr. 3.5 e 3.7) e le deroghe al consenso (par. 3.6). Il Regolamento è richiamato soltanto quale parametro sostanziale per definire consenso e informazione, in forza del rinvio operato dalla stessa normativa di settore (art. 2, lett. f), della direttiva ePrivacy; art. 94, par. 2, del Regolamento), e non è oggetto di autonoma contestazione (par. 3.4). Le ragioni per cui la contestazione riguarda i commi 1 e 2 e non il comma 2-bis sono illustrate al par. 3.2. del presente provvedimento.

La ratio dell'art. 122 e il bene giuridico tutelato. Il metodo appena illustrato impone di chiarire, prima di ogni altra valutazione, quale interesse il legislatore abbia inteso proteggere con l'art. 122 del Codice e con la disposizione europea che esso recepisce, perché è alla luce di tale finalità che vanno misurate sia la portata della norma sia la consistenza delle difese della Società. Invero, la disposizione non è una norma sul trattamento dei dati personali in senso stretto, ma una norma a presidio dell'integrità della sfera privata dell'utente: essa subordina a una scelta libera e consapevole dell'utente ogni ingresso, da parte di soggetti diversi da lui stesso, nell'apparecchio terminale di cui dispone e nelle informazioni che vi sono custodite.

Tale è la prospettiva della direttiva ePrivacy, il cui considerando 24 afferma che le apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature costituiscono parte della sfera privata degli utenti, che richiede protezione ai sensi della Convenzione europea dei diritti dell'uomo, e che i cosiddetti software spia, "*web bugs*", identificatori occulti e altri dispositivi analoghi possono introdursi nel terminale dell'utente a sua insaputa al fine di avere accesso a informazioni, archiviare informazioni occulte o seguire le attività dell'utente, e possono costituire una grave intrusione nella vita privata di tale utente; l'uso di tali dispositivi, aggiunge il considerando, "*dovrebbe essere consentito unicamente per scopi legittimi e l'utente interessato dovrebbe esserne a conoscenza*". Al riguardo, la Corte di giustizia ha precisato che l'art. 5, par. 3, "*fa riferimento all''archiviazione di informazioni' e all''accesso a informazioni già archiviate', senza qualificare tali informazioni né precisare che queste debbano essere dati personal*i", e che la disposizione "*mira dunque a proteggere l'utente da qualsiasi ingerenza nella sua vita privata, indipendentemente dal fatto che detta ingerenza riguardi o meno dati personali*" (Planet49, punti 68-69). Richiamando il considerando 24, la Corte ha aggiunto che tale tutela "*si applica a qualsiasi informazione archiviata in tale apparecchiatura terminale*" ed è volta a tutelare gli utenti dal rischio che identificatori occulti o altri dispositivi analoghi si introducano nel terminale "*a sua insaputa*" (punto 70).

La tutela nell'ordinamento nazionale e i beni protetti. Il legislatore nazionale ha fatto propria la medesima prospettiva: la relazione illustrativa allo schema del d.lgs. 28 maggio 2012, n. 69 (di seguito "relazione illustrativa") spiega che la riforma dell'art. 122 mira a far sì che gli utenti siano "*maggiormente informati*" su ciò che accade ai loro dati e possano "*esercitare più facilmente un controllo su di essi*". I beni protetti sono dunque due, strettamente connessi: la riservatezza del terminale e delle informazioni in esso contenute, e l'autodeterminazione dell'utente, cioè la possibilità effettiva di sapere chi accede al proprio dispositivo, a quali informazioni, per quali scopi, e di scegliere se consentirlo. Gli Orientamenti 2/2023 dell'EDPBpb sintetizzano tale duplice tutela affermando che la direttiva protegge la privacy degli utenti "*non solo in relazione alla riservatezza delle loro informazioni, ma anche salvaguardando l'integrità dell'apparecchiatura terminale*" (par. 14; v. anche par. 8). Da tale finalità discende che la tutela è anticipata e prescinde dalla prova di un danno, dalla trasmissione delle informazioni e dalla loro natura più o meno sensibile (v. par. 3.3). **Il rischio concreto emerso dall'istruttoria.** Alla luce di tale finalità, l'istruttoria ha evidenziato un rischio concreto per i beni protetti. La Relazione tecnica ha rilevato che le autorizzazioni READ_MEDIA richieste dall'app, concesse con un'unica finestra di sistema nella forma "Consenti tutto", abilitano Meta a leggere l'intero archivio fotografico e video del dispositivo, a elaborarlo localmente o in cloud e, poiché l'app dispone anche dell'autorizzazione INTERNET, a trasmetterlo ai propri sistemi; che l'accesso concesso è di regola permanente e revocabile solo dalle impostazioni del dispositivo; che l'autorizzazione sulle foto può comprendere, senza una seconda richiesta, quella ai metadati di ubicazione (ACCESS_MEDIA_LOCATION); e che l'app è un software chiuso, con traffico cifrato, sicché né l'utente, né l'Autorità, sono in grado di verificare quali informazioni siano effettivamente lette e trasmesse, e l'accertamento è rimesso sotto il profilo tecnico alla più ampia collaborazione del titolare. Deve infatti osservarsi che l'archivio multimediale di uno smartphone è tra i luoghi più intimi della vita digitale di una persona: conserva immagini e video della vita privata e familiare, spesso anche di terzi e di minori, che l'utente non ha mai inteso rendere accessibili a un fornitore di servizi. Va tuttavia precisato che l'Autorità non ha accertato che la Funzionalità acceda a dati di ubicazione, che i contenuti siano trasmessi o utilizzati per scopi ulteriori, né che siano trattate categorie particolari di dati, e tali ipotesi non sono poste a fondamento della decisione. Ma l'istruttoria ha mostrato, e la Società non ha smentito con alcun elemento tecnico, che le condizioni per tali esiti sono state create da Meta: un accesso ampio, continuativo e non verificabile, ottenuto attraverso un'autorizzazione richiesta per altri scopi e priva di un consenso specifico per la Funzionalità. È questo il pericolo per la sfera privata dell'utente che l'art. 122 intende prevenire.

Accesso ampio e continuativo. Nel prosieguo, per accesso "ampio" si intende quello reso tecnicamente possibile dalle autorizzazioni READ_MEDIA concesse nella forma "Consenti tutto", che abilitano l'app a leggere tutte le fotografie e i video presenti sul dispositivo e non soltanto quelli scelti dall'utente (Relazione

tecnica, par. 1.1); per "continuativo" si intende che l'autorizzazione, una volta concessa, resta di regola valida fino alla revoca esplicita dell'utente nelle impostazioni di sistema (ivi, par. 1.1 e nota 3), e non che la Funzionalità legga di continuo l'archivio. L'ampiezza è dunque una caratteristica dell'autorizzazione e della capacità tecnica che essa conferisce a Meta, non dell'uso che la Funzionalità ne fa, che secondo Meta si limita ai contenuti più recenti e ai metadati di base (memoria, §4.17) e che l'Autorità non è in grado di verificare.

Accesso limitato. La scelta dell'opzione "Consenti accesso limitato", introdotta con Android 14 (autorizzazione READ_MEDIA_VISUAL_USER_SELECTED), restringe l'accesso ai soli contenuti selezionati dall'utente. Per l'Autorità tale limitatezza non fa differenza: l'art. 122 si applica a qualunque accesso a informazioni archiviate nel terminale, senza limiti di durata o di quantità (Orientamenti 2/2023 dell'EDPB, par. 37); la scelta riguarda l'app nel suo complesso e non la singola Funzionalità, sicché non conferisce specificità al consenso; l'opzione non è offerta agli utenti di Android 13 e precedenti; e l'accesso al sottoinsieme resta permanente salvo revoca, mentre ogni sua modifica impone di ripetere la procedura, il che induce di fatto a concedere la più ampia autorizzazione (Relazione tecnica, par. 1.4). La limitatezza dell'accesso incide pertanto, al più, sull'intensità dell'interferenza (v. par. 6.2), non sulla sussistenza della violazione, né sui vizi di specificità e di informazione (parr. 3.5 e 3.7).

Il contenuto dell'art. 122 del Codice. L'art. 122, comma 1, del Codice, che recepisce l'art. 5, par. 3, della direttiva ePrivacy, consente l'archiviazione di informazioni nell'apparecchio terminale di un contraente o di un utente, o l'accesso a informazioni già archiviate, unicamente a condizione che l'utente abbia espresso il proprio consenso dopo essere stato informato con modalità semplificate. Il consenso può essere espresso anche mediante specifiche configurazioni di programmi informatici o di dispositivi, purché di facile e chiara utilizzabilità per l'utente (art. 122, comma 2). L'art. 122, comma 2-bis, vieta, salvo quanto previsto dal comma 1, di utilizzare una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale. Le sole deroghe al consenso sono l'archiviazione o l'accesso tecnico finalizzati unicamente alla trasmissione di una comunicazione su una rete di comunicazione elettronica e quelli strettamente necessari al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'utente. Il testo del comma 1, che secondo la relazione illustrativa riporta fedelmente quello dell'art. 5, par. 3, della direttiva come modificato dalla direttiva 2009/136/CE, vieta l'accesso a informazioni già archiviate nel terminale senza richiedere, ai fini dell'accesso, che le informazioni lascino il dispositivo, né che sia utilizzata una rete di comunicazione elettronica. Va peraltro precisato che il riferimento alla rete è proprio del solo comma 2-bis che, come emerge dai lavori preparatori (resoconto della XIV Commissione della Camera dei deputati, seduta del 17 maggio 2012, atto del Governo n. 462), conserva il divieto generale già previsto dal comma 1 nella formulazione previgente e non è oggetto della contestazione, che riguarda i commi 1 e 2.

La nozione di consenso. La nozione di consenso richiesta dall'art. 122 non è autonoma: l'art. 2, lett. f), della direttiva ePrivacy la identifica con il consenso dell'interessato definito dal Regolamento, cioè una manifestazione di volontà libera, specifica, informata e inequivocabile, resa mediante dichiarazione o azione positiva inequivocabile (art. 4, n. 11, del Regolamento), accompagnata dalle condizioni dell'art. 7 e dai considerando 32 e 43 (cfr. EDPB, "Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679", versione 1.1 del 4 maggio 2020; Planet49 e Orange România). Il consenso deve essere prestato per ciascuna finalità distinta e non può risultare dal silenzio, dall'inattività o da opzioni preselezionate.

Il carattere preventivo e attivo del consenso e dell'informazione. L'art. 5, par. 3, della direttiva e l'art. 122, comma 1, del Codice richiedono che l'utente sia informato e presti il consenso prima dell'accesso e che il consenso risulti da un comportamento attivo e non possa essere presunto: prima l'informazione, poi il consenso, poi l'accesso. Gli sviluppi giurisprudenziali e la loro applicazione al caso di specie sono svolti nei parr. 3.5 e 3.7 del presente provvedimento.

Gli Orientamenti 2/2023 e la loro autorità interpretativa. L'ambito tecnico dell'art. 5, par. 3, della direttiva è chiarito dagli Orientamenti 2/2023 dell'EDPB, secondo cui la disposizione si applica ogniqualvolta un'entità adotta misure per ottenere l'accesso a informazioni archiviate nel terminale, a prescindere dall'origine delle informazioni e, tipicamente, quando invia istruzioni al terminale per riceverne indietro le informazioni (par. 30-33); l'uso locale di informazioni da parte di un'applicazione tramite API di sistema non integra un accesso fintanto che le informazioni non lasciano il dispositivo, ma quando si accede a tali informazioni o a qualsiasi loro derivato, si applicherebbe l'articolo 5, paragrafo 3, della predetta direttiva

(par. 44); l'elaborazione locale e il codice lato client sono rilevanti quando le informazioni trattate sono rese disponibili a terzi, ad esempio inviate a un server su istruzione dell'entità che fornisce il codice (par. 52-53); l'applicabilità della disposizione non implica automaticamente l'obbligo di consenso, occorrendo verificare se ricorra una deroga (par. 56). L'art. 122 del Codice non è peraltro limitato ai c.d. strumenti di tracciamento: la disposizione disciplina l'accesso a informazioni già archiviate, quale che sia la tecnologia utilizzata (cfr. Linee guida cookie e altri strumenti di tracciamento del 10 giugno 2021, in www.gpdp.it doc. web n. 9677876). Gli Orientamenti 2/2023 costituiscono un atto di *soft law* dell'EDPB: sono un autorevole ausilio interpretativo, che l'Autorità considera e discute puntualmente (v. infra), ma non vincolano l'applicazione dell'art. 122, la cui portata si determina in base al testo della disposizione e della direttiva che essa recepisce, alla loro finalità e alla giurisprudenza della Corte di giustizia, e non può essere ristretta per via interpretativa da indicazioni che il testo non contiene.

Prova, informazione e sanzioni. Sotto il profilo probatorio, il titolare deve essere in grado di dimostrare la conformità dei trattamenti e di aver ottenuto un consenso valido (artt. 5, par. 2, e 24 del Regolamento). Per l'informazione, gli artt. 12 e 13 del Regolamento forniscono i parametri di sinteticità, trasparenza, intelligibilità e accessibilità con cui si misura l'informazione "*con modalità semplificate*" dell'art. 122, comma 1, del Codice. Quanto alle sanzioni, la violazione dell'art. 122 del Codice è punita ai sensi dell'art. 83, par. 5, del Regolamento (art. 166, comma 2, del Codice). Tale impianto è coerente con l'art. 15 bis della direttiva, che impone agli Stati membri di determinare sanzioni effettive, proporzionate e dissuasive per la violazione delle norme nazionali di attuazione (par. 1), di attribuire all'autorità competente il potere di ordinare la cessazione delle violazioni (par. 2) e di munirla delle competenze necessarie, compreso il potere di ottenere ogni informazione pertinente (par. 3).

3.2 Tempestività, contraddittorio, genericità della contestazione e individuazione del titolare

I rilievi sul contraddittorio. L'Autorità ha esaminato gli atti istruttori (la segnalazione, la richiesta di informazioni e la risposta di Meta, la Relazione tecnica, l'atto di avvio) e la memoria difensiva, che ha considerato integralmente, anche con riguardo ai profili sui quali Meta ha riservato di non riconoscere la competenza dell'Autorità. Il contraddittorio è stato pienamente garantito: Meta ha avuto accesso all'intero fascicolo, ha ottenuto una proroga di quarantacinque giorni oltre il termine ordinario di trenta giorni (art. 166, comma 6, del Codice) e, quando ha rappresentato di non aver potuto leggere gli allegati inviati in formato compresso, per una peculiarità dei propri sistemi, la documentazione le è stata ritrasmessa con congruo anticipo rispetto alla scadenza.

L'asserita genericità della contestazione. L'atto di avvio contesta la violazione dell'art. 122 del Codice e, dopo aver descritto in dettaglio i fatti (par. 2 e 3), ne illustra le ragioni di illiceità in distinti profili: l'assenza di un consenso specifico per la Funzionalità e distinto da quello relativo alle altre funzionalità dell'app; l'inidoneità delle basi giuridiche invocate da Meta; la carenza di informazione agli utenti già attivi e di informazioni specifiche nell'informativa e nel prodotto; le modalità di richiesta di autorizzazione (par. 4). Il riferimento agli artt. 6, 7, 12 e 13 del Regolamento, introdotto dalla locuzione "*anche in relazione*", richiama i parametri sostanziali con cui, per effetto dell'art. 2, lett. f), della direttiva ePrivacy e dell'art. 122, comma 1, del Codice, si misura il consenso e l'informazione dell'utente. La contestazione, dunque, ha consentito alla Società di individuare il fatto e le norme asseritamente violate, come dimostra la puntualità con cui Meta ha replicato a ciascun profilo (par. 2.2). Deve pertanto respingersi l'eccezione preliminare restando fermo che, per le ragioni esposte al par. 3.4, non sono accertate violazioni autonome delle disposizioni del Regolamento.

La perimetrazione della contestazione. L'atto di avvio contesta la violazione dell'art. 122, commi 1 e 2, del Codice e non anche quella del comma 2-bis. I commi 1 e 2 contengono la regola di condotta che qui rileva: l'archiviazione di informazioni nel terminale e l'accesso a quelle già archiviate sono consentiti unicamente a condizione che l'utente abbia espresso il proprio consenso dopo essere stato informato, secondo le modalità stabilite dalla stessa disposizione. L'Autorità ha quindi ancorato la contestazione a ciò che è tecnicamente provato e non è contestato dal titolare: la capacità dell'app di accedere, in forza dell'autorizzazione concessa, al contenuto multimediale del terminale, in assenza di un consenso specifico e di un'informazione adeguata. La delimitazione risponde al principio di corrispondenza tra contestazione e decisione, che impone all'Autorità di pronunciarsi solo sui fatti e sulle norme contestati alla Società nell'atto di avvio, a garanzia del suo diritto di difesa (art. 166, commi 5 e 6, del Codice). Tale scelta non vale ad escludere che il comma 2-bis concorra a definire l'ambito della tutela, né ad attenuare la gravità della condotta, che è la stessa e che resta integralmente riconducibile all'art. 122, commi 1 e 2; essa evita soltanto di spostare il confronto su un

elemento, l'uso della rete, che non è necessario per integrare la violazione e sul quale la Società ha tentato di ricondurre l'intera controversia, nonostante non abbia fornito elementi tecnici dirimenti.

L'individuazione del titolare. Quanto all'individuazione del titolare, l'atto di avvio reca, per refuso materiale, la denominazione Meta Platforms *Technologies* Ireland Limited. Meta Platforms Ireland Limited ha però dichiarato di essere il titolare del trattamento competente per la Funzionalità e il soggetto al quale erano state indirizzate la richiesta di informazioni e le comunicazioni successive; ha ricevuto l'atto di avvio, ha esercitato il diritto di accesso e ha svolto compiutamente le proprie difese, senza dedurre alcun pregiudizio. L'errore non ha pertanto inciso sul diritto di difesa. Ne consegue che il presente provvedimento è adottato nei confronti di Meta Platforms Ireland Limited.

3.3 Applicabilità dell'art. 122 del Codice, competenza del Garante sulla base della direttiva ePrivacy e non applicazione del meccanismo di cooperazione e coerenza previsto dal regolamento

Sebbene dall'intera istruttoria si evinca che l'impostazione scelta da Meta sottenda un inquadramento della Funzionalità esclusivamente dal punto di vista degli obblighi del Regolamento (ad esempio, si vedano le basi legali richiamate nell'informativa), l'Autorità, alla luce di quanto analizzato, ritiene debba trovare piena applicazione la disciplina speciale di cui alla direttiva ePrivacy e la corrispondente normativa interna di recepimento.

Ciò premesso, il perimetro dell'accertamento è circoscritto alla fase di accesso alle informazioni archiviate nel terminale e al relativo consenso e informazione (art. 122 del Codice). Gli artt. 6, 7, 12 e 13 del Regolamento sono richiamati solo quali parametri sostanziali (art. 2, lett. f), della direttiva) e non costituiscono oggetto di autonoma contestazione, così come i principi e gli obblighi generali del Regolamento richiamati nel prosieguo ai soli fini interpretativi e probatori (v. par. 3.4).

Le tesi di Meta. Con il proprio atto difensivo, Meta ha sostenuto che "*il Garante non è competente a vigilare e svolgere attività di enforcement nei confronti di Meta in relazione alla funzionalità, poiché l'art. 122 del codice (e, per estensione, l'articolo 5(3) della Direttiva ePrivacy) non trova applicazione*".

A sostegno della sua posizione, Meta richiama, sotto un profilo giuridico, i paragrafi 23, 32 e 44 degli "*Orientamenti 2/2023 sull'ambito di applicazione tecnico dell'articolo 5, paragrafo 3, della direttiva e-privacy*" (Versione 2.0, adottati il 7 ottobre 2024 dall'EDPB), enfatizzando il passaggio che indica la necessità che le informazioni debbano lasciare il dispositivo perché vi sia *accesso a informazioni già memorizzate*.

Inoltre, la Società sostiene che mancherebbe anche la trasmissione su rete di comunicazione elettronica, in quanto nel caso di specie saremmo di fronte ad una applicazione che in locale interagisce con i dati archiviati, costituendo "*un servizio basato su software, e non già una rete di comunicazione elettronica ai sensi dell'art. 5(3) della Direttiva ePrivacy*".

Sotto un profilo funzionale, Meta afferma che l'irrilevanza dell'art. 122 del Codice al caso di specie sarebbe provata dal fatto che la Funzionalità:

- operando esclusivamente *on-device*, procede alla lettura della galleria fotografica e dei relativi metadati (limitatamente a data e ora) ivi memorizzati, al fine di suggerire all'utente i contenuti multimediali più recenti da pubblicare su Facebook;

- durante tale processo i *server* di Meta non raccoglierebbero né memorizzerebbero alcun dato relativo alla galleria;

- il trattamento relativo alla Funzionalità si conclude col suggerimento di pubblicazione all'utente; e

- la pubblicazione costituirebbe una fase distinta e successiva (c.d. "Fase di Pubblicazione"), avviata dall'utente.

Le obiezioni di Meta, che si fondano sull'asserita assenza di una rete, sulla necessità che le informazioni lascino il dispositivo e sul carattere esclusivamente locale della Funzionalità, sono esaminate nell'ordine che segue: l'ambito di applicazione dell'art. 122 del Codice; la sussistenza dell'accesso nel caso di specie; le

dichiarazioni con cui Meta stessa smentisce la premessa del trattamento solo locale; la prova dell'assenza di trasmissione; infine, la competenza dell'Autorità e la non applicazione del meccanismo di cooperazione e coerenza.

L'ambito di applicazione dell'art. 122 del Codice. Sotto un profilo sistematico, lo smartphone nel quale sono conservate le foto e i video degli utenti costituisce a tutti gli effetti un'apparecchiatura terminale di rete ai sensi della normativa europea e nazionale. La circostanza, poi, che le informazioni siano generate e inizialmente conservate in locale non vale, sotto tale profilo, ad escludere l'applicabilità dell'art. 122 del Codice in materia di protezione dei dati personali, né dell'art. 5, par. 3 della direttiva ePrivacy, in quanto l'accesso a tali informazioni avviene tramite meccanismi informatici, le API del sistema operativo Android dichiarate nel file Manifest e che abilitano tecnicamente Meta ad accedere alle informazioni presenti sul dispositivo, nonché ad una successiva trasmissione in rete. Il file Manifest dichiara la capacità tecnica di accesso dell'applicazione (autorizzazioni READ_MEDIA_IMAGES e READ_MEDIA_VIDEO); la sua effettiva attivazione dipende dalla concessione dell'autorizzazione da parte dell'utente, circostanza che Meta stessa riconosce (v. infra, par. 3.5). Gli Orientamenti 2/2023 dell'EDPB annoverano espressamente lo smartphone tra le apparecchiature terminali (par. 17).

La nozione di rete di comunicazione elettronica. Non rileva che Meta qualifichi l'app come "*servizio basato su software*" e non come rete di comunicazione elettronica. L'art. 5, par. 3, nella versione vigente, non subordina l'applicazione della norma all'uso di una rete per accedere alle informazioni: l'EDPB ha osservato che la modifica del 2009 ha eliminato proprio il riferimento all'"*uso della rete di comunicazione elettronica*", estendendo la protezione dei terminali (Orientamenti 2/2023, par. 15). Allo stesso modo, l'art. 122, comma 1, del Codice, che recepisce la disposizione, non contiene alcun riferimento alla rete, che compare soltanto nel comma 2-bis, non oggetto di contestazione. L'accesso è inoltre realizzato da un software che Meta distribuisce sul terminale e che opera secondo le istruzioni da essa predisposte, ipotesi che l'EDPB ricomprende tra quelle di accesso (par. 32 e 33); e la Relazione tecnica descrive l'app come un client "*continuamente connesso con il cloud di Meta*". Del resto, la nozione di rete di comunicazione elettronica richiamata da Meta è neutra rispetto alle tecnologie di trasmissione e abbastanza ampia da coprire qualsiasi tipo di infrastruttura (Orientamenti 2/2023, par. 23-24), sicché la tesi della Società non trova riscontro neppure sul piano definitorio.

Gli Orientamenti 2/2023 dell'EDPB vanno letti per intero, e non soltanto nel passaggio invocato dalla Società. Essi precisano, anzitutto, che l'applicabilità dell'art. 5, par. 3, non si esaurisce nell'ipotesi della trasmissione, ma sussiste ogniqualvolta l'entità adotta misure per ottenere l'accesso alle informazioni archiviate (par. 32), come avviene con l'acquisizione, in sede di primo utilizzo dell'app, di un'autorizzazione ampia e permanente, nella forma "Consenti tutto" che la richiesta di sistema induce a scegliere, all'intero archivio multimediale (Relazione tecnica, par. 1.1 e 1.4); che la nozione di informazione non dipende dalla fonte né dal modo in cui le informazioni sono state conservate (par. 12, 31 e 39), che non vi sono limiti di durata o di quantità (par. 37), che la protezione non dipende dalla consapevolezza dell'utente (par. 20) e che il consenso è richiesto anche quando si accede a un valore di sola lettura mediante l'API del sistema operativo (par. 11, che richiama il parere 9/2014 del Gruppo di lavoro Articolo 29 ("WP29") sulle impronte digitali dei dispositivi). Quanto al par. 44, esso afferma che l'impiego di informazioni da parte di un'applicazione locale tramite le API di sistema non costituirebbe un "accesso" "*fintanto che le informazioni non lasciano il dispositivo*", ma aggiunge che "*quando si accede a tali informazioni o a qualsiasi loro derivato, si applicherebbe l'articolo 5, paragrafo 3*". Il passaggio non può quindi essere letto come un'esenzione generale per le applicazioni che leggono i file locali: riguarda l'ipotesi di un utilizzo strettamente interno al terminale connesso a esigenze di stretta necessità, condizione di fatto che la Società non ha dimostrato (v. infra); fa salvo l'accesso alle informazioni "*o a qualsiasi loro derivato*", quali i *suggerimenti* elaborati dalla selezione dei contenuti e dei relativi metadati compiuta dall'app, che se l'utente pubblica sulla piattaforma verrebbero comunque conosciuti da Meta; e, in ogni caso, il documento dichiara di non esaminare le deroghe (par. 4, 40 e 56).

Le caratteristiche appena ripercorse rientrano a pieno titolo nell'ambito di applicazione dell'art. 122 del Codice, quale ricostruito al par. 3.1, che subordina l'accesso a informazioni già archiviate nel terminale al consenso informato dell'utente senza richiedere che le informazioni lascino il dispositivo né che sia utilizzata una rete di comunicazione elettronica.

L'accesso nel caso di specie. La Funzionalità permette a Meta di "*accedere alla galleria di immagini presente sui dispositivi degli utenti*", consentendo alla app di analizzarne i contenuti multimediali, e di presentare "*all'utente, durante la navigazione su Facebook, suggerimenti di condivisione di base provenienti dalla sua galleria*". Le fotografie, i video e i relativi metadati conservati nella memoria dello smartphone sono informazioni già archiviate nell'apparecchio terminale dell'utente, quale che ne sia l'origine. Inoltre, l'app Facebook, una volta che l'utente abbia accordato le autorizzazioni READ_MEDIA senza limitazioni ("Consenti tutto"), può leggere l'intero archivio multimediale condiviso (Relazione tecnica, par. 1.1). Peraltro, Meta stessa descrive il funzionamento della Funzionalità come una lettura di tali informazioni: la Funzionalità, verificata la presenza dell'autorizzazione di sistema e l'attivazione dell'impostazione in-app, "*interroga l'indice della galleria del dispositivo per individuare gli elementi aggiunti più di recente e ne seleziona uno al fine di generare un suggerimento di condivisione*" (memoria, §4.17). Si tratta di un accesso a informazioni archiviate nel terminale, nel senso dell'art. 122. Tale accesso è compiuto mediante il software di Meta, che legge e seleziona i contenuti, prima e a prescindere da qualsiasi scelta dell'utente. In tale contesto, la finalità naturale ed espressamente dichiarata di tale Funzionalità è la pubblicazione del contenuto suggerito sul profilo dell'utente: diversamente, l'utilità stessa della Funzionalità sarebbe di fatto nulla. Ne consegue che il trattamento posto in essere da Meta si articola in due fasi sequenziali, di accesso ai dati memorizzati e di pubblicazione, inscindibilmente collegate, delle quali solo la prima forma oggetto di esame in questa sede.

Il modello di autorizzazioni Android. La tesi di Meta, secondo cui la Società non avrebbe accesso ai dati nell'ambito dell'operatività della Funzionalità, è smentita dal modello delle autorizzazioni del sistema Android, quello considerato nella presente istruttoria. Come riportato dalla stessa Società nelle proprie difese, "*il modello di autorizzazioni di Android non consente alle app di richiedere l'accesso ai contenuti multimediali su base individuale per ciascuna funzionalità. L'Autorizzazione a Livello di Sistema Operativo si applica all'App nel suo complesso e il perimetro rilevante ai fini di tale accesso è sempre sotto il pieno controllo dell'utente (e.g., accesso completo o accesso limitato solo a elementi selezionati)*". Quanto alla possibilità di scegliere un accesso limitato, che non muta tale conclusione, v. infra, par. 3.5. Non può quindi sostenersi che Meta abbia accesso ai contenuti multimediali degli utenti che hanno autorizzato l'app Facebook a livello di sistema operativo, mentre tale accesso non sarebbe operativo per la Funzionalità, che è integrata nella medesima app: l'autorizzazione all'accesso alla galleria opera per l'intera app. Ne consegue che l'autorizzazione generica concessa per pubblicare una foto abilita l'app, e quindi Meta, a leggere l'archivio anche per la Funzionalità. In ogni caso, per l'Autorità la limitatezza dell'accesso non fa differenza ai fini della violazione.

La "Fase di Pubblicazione". Non rileva, in contrario, che la pubblicazione del contenuto suggerito avvenga su iniziativa dell'utente (c.d. "Fase di Pubblicazione", nella definizione di Meta). L'Autorità non contesta tale fase in sé, ma l'accesso che la precede, per tre ragioni. In primo luogo, la lettura dell'archivio, la selezione del contenuto e la sua proposta all'utente sono compiute da Meta prima che l'utente abbia compiuto alcuna scelta. La successiva decisione di pubblicare interviene a valle di un accesso già avvenuto e non può integrare il consenso richiesto dall'art. 122, che deve essere preventivo, specifico e informato rispetto all'accesso stesso. Inoltre, la Funzionalità, preimpostata come attiva, opera nei confronti di tutti gli utenti che abbiano concesso l'autorizzazione di sistema, anche di coloro che non pubblicheranno mai il contenuto suggerito: per costoro l'accesso si fonda unicamente sull'autorizzazione di sistema, concessa per altro scopo, senza alcun atto volontario specificamente riferito alla Funzionalità. Infine, Meta sostiene che l'autorizzazione ha una "unica finalità", ossia facilitare la condivisione, per affermarne la validità come consenso (memoria, §4.27-4.28), e al contempo che accesso e pubblicazione sarebbero trattamenti distinti, per escludere l'applicabilità dell'art. 122 (§4.14-4.16). Le due posizioni sono inconciliabili: se la finalità è unica, l'accesso è il primo atto di un'operazione unitaria; se le fasi sono distinte, l'autorizzazione generica non copre la Funzionalità e non è specifica.

Le dichiarazioni di Meta e la premessa del trattamento solo locale. Le difese di Meta poggiano su una premessa: secondo la Società, la prima parte della Funzionalità, che va dall'accesso alla galleria alla selezione e alla proposta del suggerimento, non integrerebbe un trattamento riferibile a Meta (memoria, §4.14-4.17). Tale premessa è smentita dalle stesse informazioni che Meta ha reso all'Ufficio e agli utenti.

La nota del 14 novembre 2025. Risultano anzitutto sorprendenti, rispetto a tali premesse, le informazioni che la Società ha trasmesso con la nota del 14 novembre 2025 (prot. n. 152086/25), che ingenerano dubbi sulla coerenza delle diverse versioni fornite. A espressa domanda dell'Ufficio in merito alle basi di legittimità

del trattamento posto in essere per il tramite della Funzionalità, Meta ha affermato: "*Per il trattamento dei dati personali finalizzato a fornire la Funzionalità, Meta si basa sulla necessità di eseguire un contratto per gli utenti che hanno la capacità giuridica di stipulare un contratto vincolante e sull'interesse legittimo per gli utenti minorenni che hanno una capacità limitata di concludere un contratto vincolante*". Al di là del merito del riscontro, che verrà analizzato più avanti, se Meta non effettuasse trattamenti dei dati degli utenti attraverso la Funzionalità non vi sarebbe motivo di individuare e comunicare le relative basi di legittimità: tale obbligo sussiste solo se un trattamento effettivamente sussiste, e il trattamento sussiste nel momento in cui le informazioni ricavate da un archivio locale entrano nella sfera di operatività del titolare (diverso dal soggetto che detiene fisicamente l'archivio) che le utilizza per le finalità individuate. Meta ha inoltre riferito tali basi giuridiche al trattamento svolto "*per fornire la Funzionalità*", e non alla sola fase successiva di pubblicazione.

Le espressioni con cui Meta descrive la Funzionalità. Nella medesima nota si leggono, poi, espressioni che descrivono la prima parte della Funzionalità come attività svolta da Meta: "*Meta presenta all'utente, durante la navigazione su Facebook, suggerimenti di condivisione di base provenienti dalla sua galleria*"; "*Quando un utente concede a Meta l'accesso alla propria galleria tramite le impostazioni del dispositivo* […] *Meta ottiene accesso locale alla galleria presente sul dispositivo dell'utente* […] *Meta tratta i contenuti multimediali provenienti dalla galleria dell'utente in relazione alla Funzionalità* […] *Meta tratta, inoltre, i metadati di base relativi ai suddetti contenuti multimediali della galleria, quali la data e l'ora dello scatto, le foto contrassegnate come preferite dall'utente e la tipologia/orientamento della foto (a titolo esemplificativo, panorama, time lapse). Meta tratta queste informazioni per mostrare all'utente i suggerimenti di condivisione di base*"; e ancora: "*Nel caso in cui un utente disabiliti l'impostazione 'Suggerimenti da condividere provenienti dalla galleria' (cfr. Figura 1) senza modificare le impostazioni generali della galleria del dispositivo, Meta interrompe il trattamento delle informazioni provenienti dalla galleria dell'utente in relazione alla Funzionalità*". L'aggettivo "locale" descrive la modalità dell'accesso e non ne esclude l'imputabilità a Meta: la Società individua sé stessa, e non l'utente o il sistema operativo, quale soggetto che "ottiene accesso" e "tratta" i contenuti, e lo fa, per sua stessa descrizione, "*per mostrare all'utente i suggerimenti di condivisione*", cioè per una finalità che precede e prescinde dalla pubblicazione. Le informazioni fornite da Meta per descrivere il funzionamento della Funzionalità rivelano, dunque, attività di trattamento che la stessa Società dichiara di effettuare e che rientrano nell'ambito di operatività dell'art. 122 del Codice, in netta contraddizione con le difese articolate con le memorie.

Le informazioni fornite agli utenti. Nello stesso senso depongono le informazioni fornite agli utenti. Come riportato dalla Società nelle memorie, l'Informativa sulla Privacy, nella sezione "Quali informazioni raccogliamo?", include un menu denominato "Informazioni su app, browser e dispositivi", che illustra le informazioni presenti nei dispositivi che Meta raccoglie e riceve ("*Raccogliamo e riceviamo informazioni provenienti dai dispositivi che utilizzi e relative agli stessi nonché all'uso che ne fai. Ecco alcune delle informazioni che raccogliamo e riceviamo sui dispositivi:* […] *Informazioni che condividi con noi mediante le impostazioni del dispositivo, come posizione GPS, accesso alla fotocamera, foto e metadati correlati* […]"). Cliccando sul collegamento "metadati correlati", l'utente legge che "[…] *se ci concedi l'autorizzazione ad accedere alle foto del tuo dispositivo, raccogliamo metadati. Questi metadati provengono da e contengono informazioni sulle tue foto e i tuoi video, comprese la data e l'ora in cui li hai creati. Li usiamo per fare cose come ricordarti quando hai nuove foto da caricare*". Secondo Meta, questa formulazione, "inclusa nell'Informativa sulla Privacy già dal luglio 2022, contempla espressamente le caratteristiche della Funzionalità". Se così è, ne discende che Meta "raccoglie" i metadati delle foto, e la stessa informativa è incompatibile con la tesi di un trattamento esclusivamente locale. Delle due l'una: o i metadati sono raccolti da Meta, e l'art. 122 è applicabile; oppure non lo sono, e l'informativa, che Meta ritiene sufficiente a informare gli utenti, descrive in modo inesatto il trattamento. Anche nelle impostazioni "Suggerimenti da condividere provenienti dalla galleria" Meta informa gli utenti che "*quando autorizzi Facebook ad accedere alla galleria del tuo dispositivo per pubblicare foto e video, usiamo i metadati di base (ad es. quando sono state scattate le foto o quali sono state aggiunte ai preferiti) per fornire suggerimenti da condividere provenienti dalla tua galleria mentre navighi su Facebook*". Anche qui è Meta che "usa" i metadati, e per fornire suggerimenti all'utente, non per pubblicare.

Il trattamento riferibile a Meta. Pertanto, i trattamenti effettuati da Meta per il tramite della Funzionalità, e il fatto che la Società acceda alle informazioni archiviate nel dispositivo degli utenti, anche solo con riguardo ai metadati, risultano incontestabili sulla base delle dichiarazioni e dei documenti della stessa Società. Resta fermo, in ogni caso, che l'art. 122 non subordina la propria applicazione alla qualificazione dell'operazione

come trattamento di dati personali da parte del titolare: la disposizione protegge l'utente da "*qualsiasi ingerenza nella sua vita privata*", indipendentemente dal fatto che essa riguardi o meno dati personali (Planet49, punti 68-69). Le considerazioni che precedono rilevano dunque a confutazione della premessa di Meta e a ulteriore conferma dell'accesso, non perché da esse dipenda la sussistenza della violazione.

L'accesso a prescindere dalla trasmissione e dal danno. Va anzitutto precisato che, anche a voler ammettere che le informazioni non lascino il dispositivo, la tutela che l'ordinamento accorda agli utenti è anticipata: la norma non attende che dall'accesso derivi un uso pregiudizievole delle informazioni, né che queste siano divulgate; l'interferenza nella sfera privata si realizza già quando un soggetto terzo ottiene la possibilità di leggere il contenuto del terminale senza che l'utente lo abbia scelto e compreso. La prova di un danno concreto, invocata da Meta, non è dunque richiesta per la sussistenza della violazione, e non è condizione dell'interferenza che le informazioni siano trasmesse, perché ciò che il legislatore vuole impedire è che l'utente perda il controllo su chi accede al proprio dispositivo e con quali finalità. In secondo luogo, l'art. 122 non distingue in ragione della natura più o meno sensibile delle informazioni: l'intensità dell'interferenza può rilevare ai fini della sanzione, non dell'esistenza della violazione. Non può pertanto condividersi la lettura riduttiva della Società, che riconduce la questione alla sola sorte di "metadati di base": ciò che è in gioco non è la natura dei metadati letti, ma l'ampiezza del potere di Meta di accedere al terminale degli utenti. Per la stessa ragione la sussistenza della violazione non dipende dall'ampiezza dell'autorizzazione concessa: l'art. 122 si applica anche all'accesso a un sottoinsieme di contenuti, quale quello consentito dall'opzione "Consenti accesso limitato"; l'ampiezza rileva ai fini dell'informazione dovuta (par. 3.7) e della gravità della violazione (par. 6.2).

Peraltro, la circostanza che le informazioni non lascino il dispositivo, sulla quale Meta fonda la propria difesa, non è comunque provata, come si illustra di seguito.

L'opacità dell'app e la mancata produzione di elementi tecnici. Va infatti sottolineato che la Relazione tecnica ha rilevato che l'app è un software chiuso, il cui codice non è disponibile, e che il traffico verso i sistemi di Meta è cifrato, sicché l'Autorità non può accertare quali dati siano trasmessi. Meta, nonostante sia stata sollecitata in sede di atto di avvio del procedimento a fornire ogni documentazione idonea a escludere o limitare la propria responsabilità, si è limitata ad affermare che "nessun dato" viene trasmesso, senza produrre alcun elemento tecnico (descrizione dell'architettura, registrazioni del traffico, attestazioni o verifiche indipendenti): i documenti da 1 a 4 allegati alla memoria difensiva sono mere schermate delle interfacce. A fronte di tale carenza probatoria, l'Autorità ha evidenze delle autorizzazioni tecniche che sono dichiarate nel *Manifest* della App Facebook.

Il principio di responsabilizzazione. L'omessa produzione di elementi tecnici non è irrilevante, perché si colloca nel cuore del principio di responsabilizzazione. L'opacità di un sistema proprietario e cifrato determina un'asimmetria informativa tra chi lo progetta e lo gestisce e chi ne subisce gli effetti: è la medesima asimmetria che separa il titolare dall'interessato, il quale non è in grado di verificare quali informazioni dell'archivio fotografico siano effettivamente lette e trasmesse, e che separa il titolare dall'Autorità di controllo, la quale, come l'utente, si trova davanti a un sistema chiuso di cui conosce soltanto ciò che il titolare decide di rivelare o che può desumere dall'esterno. Sotto tale profilo, il Regolamento non ignora questa asimmetria, ma ne trae la conseguenza opposta a quella prospettata da Meta: poiché solo il titolare conosce e controlla l'architettura del trattamento e dispone dei mezzi per documentarla, spetta a lui dimostrare la conformità (artt. 5, par. 2, e 24 del Regolamento) e collaborare con l'Autorità fornendo le informazioni richieste (art. 31 del Regolamento; art. 157 del Codice). Per sistemi di questo tipo l'Autorità necessita della più ampia collaborazione del titolare, che è tenuto a fornire elementi tecnici idonei a riscontrare le proprie affermazioni. Il titolare non può, dunque, avvalersi a proprio vantaggio di un'opacità che deriva dalle sue stesse scelte tecniche: se così fosse, la riservatezza del codice e della cifratura diventerebbe uno schermo capace di sottrarre il trattamento a ogni verifica, e il vantaggio informativo di cui Meta dispone nei confronti degli utenti si estenderebbe, con ben maggiore effetto, all'Autorità chiamata a tutelarli. La medesima asimmetria si ripropone, moltiplicata, per la platea degli utenti interessati, che, secondo la stima di cui al par. 3.8, è nell'ordine di milioni di persone.

Non si tratta di invertire l'onere di accertare l'accesso, che l'Autorità ha provato sulla base delle autorizzazioni dichiarate dall'app, della Relazione tecnica e delle stesse dichiarazioni di Meta. Si tratta di attribuire a Meta l'onere di dimostrare il fatto che essa invoca a propria esclusione, ossia che le informazioni non lascino il dispositivo, circostanza che rientra interamente nella sua sfera di conoscenza e di controllo. È

opportuno sottolineare, al riguardo, che, a fronte della imponente mole di elementi sopra richiamati (i passaggi dell'informativa e del riscontro alla richiesta di informazioni che dimostrano il trattamento da parte di Meta e le autorizzazioni adoperate dall'app, sulla cui portata v. infra), spettava a Meta descrivere "in modo analitico", come espressamente richiesto dall'Autorità, il funzionamento tecnico della Funzionalità. La risposta della Società si è invece sorprendentemente limitata a una dichiarazione apodittica, non provata e non verificabile, nonché in contrasto con quanto precedentemente dichiarato (con il vincolo dell'art. 168 del Codice), rispetto alla quale l'Autorità dovrebbe limitarsi a un atto di fede.

Il passaggio della Relazione tecnica invocato da Meta. Né vale il passaggio della Relazione tecnica, richiamato da Meta, secondo cui la Funzionalità sarebbe "teoricamente realizzabile" senza che i dati lascino il dispositivo: la mera possibilità teorica non prova che essa sia così realizzata, e il medesimo passaggio rileva che, "all'atto pratico", le autorizzazioni adoperate dall'app abilitano Meta ad accedere a tutte le foto e ai relativi metadati e a trasmetterli senza che l'utente ne abbia contezza.

Alla luce di quanto precede l'Autorità ritiene che l'accesso alle informazioni archiviate nel terminale, nel senso dell'art. 122 del Codice, ricorra nel caso di specie. La Funzionalità è una parte di un'operazione unitaria (acquisizione di un'autorizzazione ampia all'archivio multimediale, selezione dei contenuti, suggerimento e trasmissione a Meta del contenuto scelto) che Meta stessa descrive come perseguente un'unica finalità e di cui non ha provato, né offerto di provare, che le informazioni dell'archivio non siano rese disponibili a Meta prima della pubblicazione. Ciò vale a prescindere dalla volontarietà della successiva pubblicazione, che non incide sulla fase di accesso né sulla necessità del consenso preventivo.

La competenza del Garante e la non applicazione dello sportello unico. Sul piano della competenza, Meta stessa riconosce che la direttiva ePrivacy non prevede un meccanismo di sportello unico e che il Garante è competente a farne rispettare le norme di recepimento ove applicabili (memoria, §4.1): la questione di competenza si risolve dunque interamente in quella dell'applicabilità dell'art. 122.

Il parere 5/2019 e la sentenza Facebook Belgium. La stessa documentazione richiamata da Meta conferma questa conclusione. Nel parere 5/2019 l'EDPB ha chiarito che l'autorità designata dalla legge nazionale come competente ai sensi della direttiva ePrivacy dispone della competenza per la diretta applicazione delle norme nazionali di recepimento (par. 77 e 90); che l'art. 5, par. 3, contiene una norma speciale per l'archiviazione e l'accesso alle informazioni nel terminale (par. 75); che i meccanismi di cooperazione e coerenza del Regolamento "*non si applicano all'attuazione delle disposizioni contenute nella direttiva e-privacy in quanto tali*" (par. 80 e 91); e che restano soggetti al Regolamento, e quindi allo sportello unico, i trattamenti anteriori e successivi non disciplinati da una norma speciale della direttiva (par. 75 e 84). Analogamente, nella sentenza Facebook Belgium, richiamata da Meta, la Corte, ricordando proprio il parere 5/2019, ha riferito che "*la memorizzazione e la lettura di dati personali mediante cookie rientravano nell'ambito di applicazione della direttiva 2002/58/CE* […] *e non nel meccanismo dello 'sportello unico'*", mentre le operazioni precedenti e le successive attività di trattamento rientrano nel Regolamento (Facebook Belgium, punto 74). Tale ripartizione è coerente con il perimetro dell'accertamento, che l'Autorità ha circoscritto alla fase di accesso (v. supra) senza incidere sulla competenza dell'autorità irlandese per i trattamenti successivi, che non esamina.

I poteri dell'Autorità e il "*ne bis in idem*". Quanto ai poteri, l'EDPB ha rilevato che l'autorità designata per l'attuazione della direttiva ePrivacy non può avvalersi automaticamente dei poteri del Regolamento, ma deve trovare nella legge nazionale i propri compiti e poteri (par. 66): nell'ordinamento italiano essi sono previsti dagli artt. 157 e 166 del Codice, che rinviano ai correlati poteri di cui all'art. 58, parr. 1 e 2, del Regolamento. Quanto all'esigenza di coerenza tra autorità competenti per i due strumenti, volta a evitare violazioni del principio del "*ne bis in idem*" (par. 78), essa è soddisfatta nel caso di specie, perché oggetto di contestazione è la sola violazione dell'art. 122 in relazione agli utenti italiani che hanno installato l'app Facebook in un *device* avente sistema operativo Android.

L'Autorità italiana è pertanto competente, ai sensi del Codice, ad accertare la violazione dell'art. 122 nei confronti degli utenti italiani di Facebook su dispositivi Android, perimetro cui l'atto di avvio ha circoscritto la contestazione.

3.4 Applicazione del Regolamento nel caso di specie

Meta contesta i profili di violazione prospettati da questa Autorità in merito alla base di legittimità del trattamento e all'informativa, sostenendo che "*il Garante non ha giurisdizione né competenza in merito all'applicazione e/o a vigilare sul rispetto del GDPR da parte di meta in relazione alla funzionalità*".

La Società ha affermato, inoltre, che ogni trattamento effettuato in relazione alla Funzionalità rientri nell'ambito di operatività del Regolamento e, dunque, sottenda la competenza dell'Autorità di garanzia irlandese.

L'equivoco in cui è incorso Meta è legato al fatto che, secondo la ricostruzione offerta dalla Società, il Garante pretenderebbe di verificare la conformità dei trattamenti oggetto di analisi alle disposizioni di cui agli artt. 6, 7, 12 e 13 del Regolamento.

Tale eccezione non coglie nel segno ed è, con ogni evidenza, frutto di un fraintendimento.

In realtà, il Garante ha inteso contestare esclusivamente le violazioni dell'art. 122 del Codice, anche sotto il profilo della base di legittimità e dell'informativa prevista dalla stessa norma richiamata.

Il contenuto dell'atto di avvio. Nel proprio atto di avvio del procedimento *ex* art. 166 del Codice, il Garante ha, infatti, prospettato la possibile violazione dell' "*art. 122, commi 1 e 2, del Codice, anche in relazione agli artt. 6, 7, 12 e 13 del regolamento (UE) 2016/679, per aver effettuato accessi ad informazioni archiviate nei dispositivi telefonici mobili degli utenti, segnatamente immagini fotografiche, video e relativi metadati, in assenza del richiesto consenso, o di altra valida base di legittimità, e senza aver informato gli utenti stessi secondo metodologie che assicurino la loro effettiva consapevolezza*".

Tra l'altro è la stessa formulazione dell'art. 122 del Codice che richiama il "*consenso*" come base di legittimità dei relativi trattamenti, consenso che l'utente può prestare "*dopo essere stato informato con modalità semplificate*".

Dal punto di vista sistematico, appare opportuno richiamare la formulazione della direttiva ePrivacy che all'art. 2, par. 2 lett. f) non definisce direttamente il "*consenso*" ma rinvia espressamente a quanto previsto dalla allora "*direttiva 95/46/CE*" (oggi Regolamento).

Inoltre, la formulazione dell'art. 5, par. 3 afferma che "*l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva 95/46/CE, tra l'altro sugli scopi del trattamento*".

Dunque, è la stessa normativa di riferimento che, al fine di fornire contenuti ai concetti richiamati dall'art. 122 del Codice, per il tramite dell'art. 5, par. 3 della direttiva ePrivacy, rinvia a quanto previsto dal Regolamento in relazione, nel caso di specie, al base di legittimità del consenso dell'interessato e all'informativa.

Pertanto, lungi dal volersi ritenere competente per l'applicazione del Regolamento in trattamenti transfrontalieri di cui sono competenti altre Autorità, il Garante ha contestato a Meta esclusivamente la possibile violazione dall'art. 122 del Codice in relazione agli utenti italiani. I richiami agli articoli del Regolamento, al pari di quelli effettuati dalla direttiva ePrivacy, sono dunque semplicemente esplicativi dei precisi profili dell'art. 122 del Codice che si ritengono violati, come risulta chiaro anche dalla formulazione dei relativi passaggi dell'atto di avvio del procedimento *ex* art. 166 del Codice.

La giurisprudenza della Corte di giustizia sul consenso. Tale impostazione è conforme alla giurisprudenza della Corte di giustizia, secondo cui il consenso di cui all'art. 2, lett. f), e all'art. 5, par. 3, della direttiva ePrivacy va letto in combinato disposto con la nozione di consenso della direttiva 95/46 e, oggi, con l'art. 4, punto 11, e l'art. 6, par. 1, lett. a), del Regolamento (Planet49, punti 50, 57 e 60-63). Il rinvio a tali nozioni serve a dare contenuto al requisito del consenso previsto dall'art. 122 e non trasforma la contestazione in una contestazione del Regolamento. Nello stesso senso, l'art. 1, par. 2, della direttiva ePrivacy stabilisce che le sue disposizioni "*precisano e integrano*" la direttiva 95/46, i cui riferimenti si intendono oggi fatti al Regolamento (art. 94, par. 2), e l'EDPB ha chiarito che i requisiti del consenso del Regolamento non costituiscono un "*obbligo supplementare*" ai sensi dell'art. 95, bensì condizioni preliminari di liceità,

applicabili alle situazioni che rientrano nella direttiva ePrivacy (Linee guida 5/2020, par. 7; v. anche parere 5/2019, par. 40).

La competenza dell'Autorità e quella dell'autorità capofila. Né il richiamo a nozioni del Regolamento sottrae la valutazione a questa Autorità. La Corte di giustizia ha affermato, in un contesto diverso ma significativo, che nessuna disposizione del Regolamento vieta a un'autorità che agisce sulla base di una competenza propria di constatare, nell'esercizio delle sue funzioni, la non conformità di un trattamento a tale Regolamento, e che, così facendo, essa non si sostituisce alle autorità di controllo né esercita i compiti e i poteri che il Regolamento riserva a queste ultime (Sentenza 4 luglio 2023, C-252/21, Meta Platforms e altri (Bundeskartellamt), punti 43, 48 e 49). A maggior ragione, l'Autorità che applica una norma nazionale di recepimento della direttiva ePrivacy e non adotta alcuna misura sul fondamento del Regolamento non invade la competenza dell'autorità capofila. L'Autorità è consapevole del dovere di leale cooperazione richiamato dalla Corte nella medesima sentenza, che riguarda l'autorità chiamata ad applicare il Regolamento (punti 52-54) e il comportamento già oggetto di una decisione o di un esame da parte dell'autorità competente (punti 56-57 e 63): profili che, nel caso di specie, non ricorrono.

In ogni caso, si anticipa sin d'ora, che il Garante provvederà a comunicare alla DPC il presente provvedimento per le eventuali verifiche di competenza che la stessa Autorità irlandese ritenesse necessarie.

3.5. Il consenso

La tesi di Meta. Meta sostiene che, in ogni caso, l'autorizzazione di sistema operativo costituisce un'azione positiva dell'utente, che il consenso così espresso è libero, specifico, informato e inequivocabile, che esso è riferito a un'unica finalità e che è revocabile, e che l'impostazione in-app non è un meccanismo di consenso. Tale tesi viene espressa come ipotesi subordinata rispetto a quella principale dell'inapplicabilità dell'art. 122 del Codice, evidenziando che anche sotto questo profilo il trattamento svolto dalla Società sarebbe legittimo. Le argomentazioni, tuttavia, non possono essere accolte.

La specificità della richiesta di autorizzazione. Al riguardo, dagli atti emerge, come già esposto sopra, che la richiesta di autorizzazione di cui fa cenno Meta non possiede i requisiti della specificità e della preventiva informazione: l'utente che intenda creare un post, una storia o un reel è indirizzato a una schermata secondo cui l'accesso alla galleria serve a "*condividere foto e video, ricevere suggerimenti sulle foto da caricare e abilitare altre funzioni*" (Relazione tecnica, figg. 7-9; Meta, memoria, §4.23.2, doc. 2), e, con un unico passaggio, alla finestra di sistema che chiede l'accesso a "*foto e video*". Si tratta di una richiesta unica per operazioni con requisiti di accesso diversi: la pubblicazione di una foto richiede un accesso occasionale, su richiesta e limitato al contenuto scelto, realizzabile, secondo la Relazione tecnica, senza autorizzazioni di sistema; la Funzionalità richiede, per sua natura, un accesso ampio e continuativo all'archivio (Relazione tecnica, par. 1.4).

Sotto il profilo in analisi, non rileva neanche che l'utente abbia la possibilità di scegliere, a livello di sistema e in relazione all'intera App Facebook, tra le opzioni "Consenti tutto", "Consenti accesso limitato" e "Non consentire". In primo luogo, tale possibilità è stata introdotta solo con l'aggiornamento di Android 14 (autunno 2023) mentre sino alla versione Android 13 non era prevista l'opzione "Consenti accesso limitato". Anche dove disponibile, l'opzione non risolve il problema: l'accesso al sottoinsieme selezionato resta permanente salvo revoca esplicita e ogni modifica del sottoinsieme impone di ripetere la procedura di concessione, il che induce di fatto l'utente ad accordare la più ampia autorizzazione possibile (Relazione tecnica, par. 1.4). Inoltre, lo si ribadisce, tale scelta ad opera dell'utente è relativa all'intera app Facebook e non è riferita alle singole e specifiche funzionalità, come confermato anche dalla Società.

Pertanto anche la scelta operata dell'utente - interagendo con la schermate di sistema - non ha il carattere della specificità in riferimento alla Funzionalità. Anche a voler ritenere che l'utente abbia scelto l'opzione "Consenti accesso limitato", la violazione non muta: per l'Autorità la limitatezza dell'accesso non fa differenza.

Le ammissioni di Meta. È del resto la stessa Società ad ammettere che la Funzionalità "*non può operare su una base 'una foto alla volta'*" (memoria, §6.2) e l'autorizzazione di sistema si applica "*all'App nel suo complesso*", mentre l'autorizzazione ACCESS_MEDIA_LOCATION è dichiarata "*per essere utilizzata da altre e distinte funzioni dell'App*" (§5.35). Meta, pertanto, conferma che la medesima richiesta di autorizzazione copre funzioni distinte e differenziate e tale richiesta di autorizzazione non può quindi avere i

connotati del consenso specifico richiesto dalla normativa, poiché la formula "*abilitare altre funzioni*" non consente all'utente di comprendere a quali ulteriori trattamenti dà accesso.

Meta richiama il considerando 32 del Regolamento e le Linee guida 5/2020 per sostenere che un unico consenso può coprire più trattamenti con la medesima finalità. È la stessa Società, quindi, a confermare che il consenso deve essere prestato distintamente per ciascuna finalità**.**

Libertà del consenso. A ciò deve tuttavia doverosamente aggiungersi che, in base a quanto indicato nel considerando 43 del Regolamento, il consenso non può definirsi "libero" se non è possibile prestare un consenso separato a distinti trattamenti. Orbene, la pubblicazione di un contenuto scelto dall'utente e la scansione dell'archivio multimediale per proporre contenuti da pubblicare sono operazioni diverse per natura, intensità e prevedibilità: nella prima l'utente sceglie il contenuto; nella seconda è Meta (tramite l'app) a individuare e selezionare i contenuti, tra tutti quelli accessibili. Accomunare entrambe nella medesima finalità di "*facilitare la condivisione*" può avvenire solo in ragione della palese genericità di tale finalità, idonea essa stessa a svuotare il requisito di specificità. Utilizzando il medesimo criterio, ogni funzione di un social network potrebbe essere ricondotta alla finalità di "condividere", che rappresenta il fine prevalente di chiunque intenda associarsi ad una community. Come rilevato dalla Relazione tecnica, la richiesta di un accesso ampio e continuativo avrebbe dovuto essere presentata in un momento diverso e collegata solo alla Funzionalità, disattivata per impostazione predefinita (par. 1.4). Al riguardo si deve sottolineare che la Relazione tecnica (par. 1.3) richiama la politica di Google LLC, società che ha creato e detiene il sistema operativo Android ed è dunque il soggetto che ne definisce il modello di autorizzazioni e le regole che gli sviluppatori sono tenuti a rispettare per distribuire le proprie app attraverso il relativo negozio, Google Play. Per le autorizzazioni a foto e video, tale politica prescrive di richiedere le autorizzazioni sensibili in modo incrementale, nel contesto in cui servono, e di ottenere nuovi consensi per scopi ulteriori. La fonte è particolarmente significativa: Google è il soggetto che ha ideato il modello di autorizzazioni Android al quale Meta riconduce l'impossibilità di richiedere un'autorizzazione per singola funzionalità (memoria, §6.1-6.3), ed è lo stesso che, con la propria politica, prescrive di richiedere le autorizzazioni sensibili in modo incrementale e nel contesto. Meta non può dunque invocare il modello di Android per giustificare una richiesta unica che la politica del suo stesso ideatore sconsiglia.

Il requisito di specificità nella giurisprudenza europea. Sul requisito di specificità la giurisprudenza europea è univoca. In particolare, la Corte ha affermato che la manifestazione di volontà deve essere "*specifica*", nel senso che "*deve riferirsi precisamente al trattamento dei dati interessati e non può essere desunta da una manifestazione della volontà avente un oggetto distinto*" (Planet49, punto 58; Orange România, punto 38). Sulla base di tale principio ha escluso che l'attivazione del pulsante di partecipazione a un gioco a premi potesse bastare a ritenere validamente espresso il consenso all'installazione di cookie (Planet49, punto 59), e ha chiesto al giudice nazionale di verificare se la sottoscrizione di un contratto, riferita a una pluralità di clausole, potesse valere come consenso specifico a una di esse (Orange România, punto 47). Lo stesso ragionamento vale nel caso in esame: l'autorizzazione di sistema concessa per pubblicare una foto non può essere desunta come consenso a un accesso ampio e continuativo all'archivio per una finalità distinta. Quanto al consenso separato per trattamenti distinti, richiamato sopra con riferimento al considerando 43, la Corte ha confermato che il consenso si presume non liberamente prestato se non è possibile prestarlo separatamente per ciascun trattamento (C-252/21, Meta Platforms e altri, punto 144), e che gli utenti devono poter rifiutare individualmente operazioni particolari di trattamento non necessarie, senza dover rinunciare all'intero servizio (punti 150-151). Le stesse Linee guida 5/2020 invocate da Meta, che ammettono un unico consenso per trattamenti distinti solo se questi hanno "*la medesima finalità*" (par. 57), richiedono altresì la granularità, cioè "*una possibilità di adesione distinta per ciascuna finalità*" (par. 60; v. anche par. 44), e indicano la specificazione della finalità come garanzia contro il "*function creep*", vale a dire "*l'estensione indebita delle funzionalità*", che rappresenta un rischio per l'interessato perché può comportare "*la perdita del controllo*" sui dati (par. 55-56). Quanto alla specificità della finalità dichiarata, una finalità vaga o generica, quale "*migliorare l'esperienza degli utenti*", non soddisfa i criteri per essere "specifica" (Linee guida 5/2020, nota 30, che richiama il parere 3/2013 del WP29 sulla limitazione della finalità).

Il contenuto generico della finestra di sistema. Deve inoltre osservarsi che la finestra di sistema ha contenuto generico ("foto e video") e il sistema operativo non conosce i trattamenti che l'app intende effettuare: l'utente resta pertanto privo di conoscenza dell'effettivo trattamento (Relazione tecnica, par. 2). Il fatto che l'autorizzazione sia un'azione positiva dell'utente non basta: l'azione positiva, per essere equiparata

ad un consenso preventivo, libero, specifico, informato e inequivocabile come richiede la norma, deve essere riferita specificamente al trattamento per cui il consenso è richiesto.

Meta riconosce che l'impostazione in-app (cioè l'interruttore presente nelle impostazioni dell'app Facebook, alla voce "Ottieni suggerimenti dalla galleria quando navighi su Facebook") non è un meccanismo di consenso (memoria, §4.31). Tale impostazione si limita ad attivare o disattivare la Funzionalità all'interno dell'app e non abilita, di per sé, alcun accesso alla galleria, che dipende dall'autorizzazione concessa a livello di sistema operativo. Resta dunque, quale unico atto dell'utente diretto a consentire l'accesso alla galleria, l'autorizzazione di sistema operativo (la finestra di Android che chiede l'accesso a "foto e video"). . Essa, tuttavia, non è specifica per la Funzionalità: viene richiesta all'utente per pubblicare una foto o un video, è concessa "*all'App nel suo complesso*" e copre, come Meta ammette, anche funzioni distinte (memoria, §5.35 e §6.2). L'utente che la concede per pubblicare un contenuto non ha quindi manifestato alcuna volontà riferita alla Funzionalità. Il consenso così espresso ha infatti un oggetto diverso e più generico, l'accesso dell'app a "foto e video", e non può essere esteso alla Funzionalità, poiché la manifestazione di volontà "*non può essere desunta da una manifestazione della volontà avente un oggetto distinto*" (Planet49, punto 58). Ne consegue che l'autorizzazione di sistemanon costituisce, rispetto alla Funzionalità, il consenso richiesto dall'art. 122, che permette l'accesso "unicamente a condizione" che esso sia stato validamente espresso. È in questi termini che va esaminato il passo della difesa di Meta nella quale la Società, pur non invocando espressamente l'art. 122, comma 2, sostiene che il consenso sarebbe espresso mediante una configurazione del dispositivo. Anche così intesa, la tesi non regge: il comma 2 consente di esprimere il consenso mediante configurazioni di facile e chiara utilizzabilità, ma presuppone pur sempre un consenso con i requisiti dell'art. 122, comma 1, e cioè informato e specifico, oltre che libero e inequivocabile. La finestra di sistema, generica per natura, non consente di esprimere un consenso avente tali caratteristiche per la Funzionalità. A ciò si aggiunge che le Linee guida 5/2020 precisano, con riferimento al consenso espresso mediante impostazioni (nell'esempio, quelle del browser), che queste devono essere sviluppate in linea con le condizioni di validità del consenso, tra cui il fatto che sia granulare per ciascuna delle finalità previste (par. 89), e che il consenso non può essere ottenuto tramite la stessa azione con cui si accetta un contratto o le condizioni generali di servizio (par. 81) né dedotto dalla semplice prosecuzione dell'uso normale (par. 84).

L'impostazione in-app attiva prima dell'autorizzazione. Va rilevato, inoltre, che Meta ha ammesso che l'impostazione in-app poteva apparire "attiva" anche prima che l'utente concedesse l'autorizzazione di sistema (memoria, §4.33), contrariamente a quanto aveva dichiarato nella risposta del 14 novembre 2025, ove l'opzione risultava "inattiva" per gli utenti che non avevano concesso l'autorizzazione. Meta riferisce di aver risolto il problema con la versione 581 dell'app, precisando tuttavia che gli utenti che non hanno effettuato l'aggiornamento continueranno a visualizzare la precedente interfaccia (memoria, nota 7).

L'avvio della Funzionalità senza una scelta dell'utente. Sotto altro profilo, Meta sostiene, e la stessa Relazione tecnica conferma, che la Funzionalità non opera finché l'utente non concede l'autorizzazione di sistema operativo. L'Autorità ne prende atto, ma ne trae una conclusione diversa da quella della Società. Secondo quanto dichiarato da Meta nella nota del 14 novembre 2025, l'impostazione in-app diventa attiva per gli utenti che hanno concesso l'autorizzazione di sistema operativo: la Funzionalità si avvia quindi quando l'utente concede tale autorizzazione, ad esempio per pubblicare una foto, senza che sia richiesto alcun ulteriore atto e senza che all'utente sia mai stata chiesta una scelta riferita ad essa. Le modifiche introdotte con la versione 581 dell'app (memoria, §4.34) riguardano la coerenza tra lo stato mostrato dall'impostazione e la capacità di accesso, e non il momento in cui la Funzionalità si attiva. Il consenso richiesto dall'art. 122 deve risultare da un'azione positiva e inequivocabile dell'utente, non dal silenzio o dall'inattività (Planet49; Orange România). È Meta stessa che riconosce che l'impostazione in-app non è un meccanismo di consenso (memoria, §4.31): essa non può dunque costituire, né nello stato "attivo" né in quello "inattivo", la manifestazione di volontà richiesta dall'art. 122, e Meta non può ricondurvi l'atto positivo che la normativa esige. Resta soltanto l'autorizzazione di sistema operativo, che l'utente concede in vista di un altro scopo, tipicamente la pubblicazione di un contenuto: l'autorizzazione vi è, ma non è riferita alla Funzionalità, rispetto alla quale l'utente non ha espresso alcuna scelta specifica.

Il "comportamento attivo" nella giurisprudenza. Tale principio è costante nella giurisprudenza. In particolare, la Corte ha precisato che il requisito della "*manifestazione*" di volontà "*evoca chiaramente un comportamento attivo e non uno passivo*" (Planet49, punto 52) e che solo un comportamento attivo è idoneo a soddisfare il requisito dell'inequivocabilità (punto 54). Con riferimento alla casella preselezionata, ha rilevato che è "*praticamente impossibile determinare in modo oggettivo*" se l'utente abbia manifestato il

consenso e se lo abbia fatto in modo informato, non potendo escludersi che non abbia letto l'informazione "*o addirittura che lo stesso non abbia visto tale casella*" (Planet49, punto 55; Orange România, punto 37). Tali principi, enunciati per la casella preselezionata, valgono a maggior ragione per una funzione che si avvia in forza di un'autorizzazione concessa per altro scopo e che l'utente non ha mai avuto occasione di scegliere né, talvolta, di vedere.

Il carattere preventivo del consenso. Quanto al carattere preventivo, il testo vigente dell'art. 5, par. 3, della direttiva richiede che l'utente abbia "*espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo* […] *tra l'altro sugli scopi del trattamento*" (Planet49, punto 46; Corte di giustizia, sentenza del 29 luglio 2019, C-40/17, Fashion ID, punti 13 e 89). La Corte di giustizia ha chiarito che tale formulazione è frutto di una scelta consapevole del legislatore europeo: la versione iniziale della disposizione prevedeva soltanto la "*possibilità di rifiutare*" l'installazione dei cookie, mentre la direttiva 2009/136/CE ha sostituito tali termini con "*espresso preliminarmente il proprio consenso*", sicché il consenso dell'utente "*non può più essere presunto e deve risultare dal comportamento attivo di quest'ultimo*" (Planet49, punto 56). Nella medesima prospettiva, la Corte ha affermato che il consenso deve essere espresso prima dell'operazione e che l'informazione deve essere fornita "*immediatamente, ossia al momento della raccolta*", a presidio di una "*tutela efficace e tempestiva dei diritti della persona interessata*" (Fashion ID, punti 102 e 104, resi con riferimento alla direttiva 95/46). La sequenza è la stessa nel testo italiano, che consente l'accesso alle informazioni già archiviate "*unicamente a condizione che*" l'utente abbia espresso il proprio consenso dopo essere stato informato: prima l'informazione, poi il consenso, poi l'accesso. Anche l'EDPB ritiene che il carattere preventivo del consenso sia "*chiaramente implicito*" nella definizione del Regolamento, in quanto il consenso deve essere espresso prima che abbia luogo l'attività di trattamento (Linee guida 5/2020, par. 90). Ne discende che l'autorizzazione deve essere preventiva e attiva, e che non può essere desunta da un comportamento passivo, né da un atto compiuto per uno scopo diverso.

Gli utenti già attivi e l'assenza di nuove notifiche. Inoltre, la Relazione tecnica ha rilevato che gli utenti che già utilizzavano l'app al momento dell'aggiornamento ad Android 13, e disponevano della precedente autorizzazione READ_EXTERNAL_STORAGE, hanno ricevuto automaticamente le autorizzazioni READ_MEDIA. Meta riferisce che l'avviso che precede la richiesta di autorizzazione compare solo agli utenti che non hanno ancora concesso l'autorizzazione (memoria, §5.32.2) e riconosce che non è stata inviata alcuna notifica ulteriore e separata (§5.31). Gli utenti che avevano già concesso l'autorizzazione prima del lancio della Funzionalità nel 2023 non hanno quindi mai ricevuto una richiesta riferita a questa, né avuto occasione di esprimere una correlata volontà, essendo l'unico atto a loro riconducibile l'autorizzazione concessa in precedenza, per altri scopi e prima dell'introduzione della Funzionalità.

La revocabilità dell'autorizzazione. Meta evidenzia, inoltre, che l'autorizzazione è revocabile (memoria, §4.24) e che un accesso revocabile non può definirsi "continuativo". L'Autorità osserva che la revocabilità attiene alla possibilità di ritirare il consenso (art. 7, par. 3, del Regolamento), non alla validità del consenso al momento in cui è prestato; e che la continuità è una caratteristica dell'accesso che l'app può effettuare finché l'autorizzazione non è revocata, non dell'impossibilità di revoca. La Relazione tecnica osserva, del resto, che nella generalità dei casi l'autorizzazione, una volta accordata, resta permanente finché l'utente non la revoca di propria iniziativa e che la revoca richiede un'azione esplicita e consapevole nelle impostazioni di sistema, pur potendo l'utente avvalersi della schermata di riepilogo messa a disposizione dall'app (par. 1.1 e nota 3). L'argomento della difficoltà di revoca del consenso non è peraltro tra le ragioni su cui il presente provvedimento e la prodromica contestazione si fondano.

L'onere della prova del consenso. Quanto all'onere della prova, la Corte ha precisato che spetta al titolare dimostrare l'esistenza di un valido consenso (Orange România, punti 42 e 51-52; C-252/21, Meta Platforms e altri, punti 95 e 152; Linee guida 5/2020, par. 104-107), che non può pretendere che gli utenti manifestino attivamente il proprio rifiuto (Orange România, punto 51) e che il mero compimento di un atto, quale la sottoscrizione di un contratto contenente una clausola, non dimostra di per sé il consenso "*in assenza di indicazioni che confermino che tale clausola è stata effettivamente letta e assimilata*" (Orange România, punto 46). Nel caso di specie Meta non ha prodotto alcun elemento da cui risulti che gli utenti, nel concedere l'autorizzazione di sistema, abbiano compreso che essa avrebbe abilitato la Funzionalità; e per gli utenti che, avendo ricevuto l'aggiornamento ad Android 13, utilizzavano già la app Facebook e detta app godeva della precedente autorizzazione READ_EXTERNAL_STORAGE, la stessa è stata automaticamente estesa alle autorizzazioni READ_MEDIA, non risultando alcun nuovo atto di volontà espressamente riferito all'accesso alla galleria né, a maggior ragione, alla Funzionalità.

In tale quadro, dunque, il consenso richiesto dall'art. 122, commi 1 e 2, del Codice non è stato validamente acquisito.

3.6. La stretta necessità e le basi giuridiche invocate

La stretta necessità invocata da Meta. Con argomentazioni subordinate, Meta afferma che l'accesso sarebbe strettamente necessario per l'erogazione di un servizio esplicitamente richiesto dall'utente, consistente nel "*processo efficiente ed efficace di caricamento delle fotografie*" (memoria, §4.37). L'argomento, svolto in un solo paragrafo e senza alcun elemento a supporto, è infondato. L'eccezione al consenso dell'art. 122, comma 1, va interpretata restrittivamente e riguarda l'accesso strettamente necessario per fornire un servizio che l'utente ha richiesto in modo esplicito.

Invero, la Funzionalità non è un servizio richiesto dall'utente ma, come afferma Meta, "*uno strumento opzionale dell'App*" (memoria, §2.2), disattivabile (§1.3.6). Il servizio effettivamente richiesto dall'utente, cioè la pubblicazione di un contenuto, può essere reso anche senza che la Funzionalità sia attiva e con un accesso limitato al contenuto scelto, come dimostra l'esistenza della funzione "photo picker"; Meta riconosce infatti che la Funzionalità richiede un accesso diverso da quello necessario per pubblicare singole foto (memoria, §6.2-6.3). L'Autorità non ha ritenuto che il "photo picker" costituisca un obbligo né ne fa un autonomo addebito, come Meta osserva (§6.1): il rilievo tecnico ha pregio quale elemento di fatto, che esclude la stretta necessità di un accesso generale all'archivio per la Funzionalità e conferma la diversità dei trattamenti.

L'interpretazione restrittiva delle giustificazioni alternative al consenso. Il rigore con cui la Corte interpreta le giustificazioni alternative al consenso conferma tale conclusione. Pur con riferimento all'art. 6 del Regolamento, la Corte ha ricordato che le giustificazioni che rendono lecito un trattamento in assenza di consenso vanno interpretate restrittivamente (C-252/21, Meta Platforms e altri, punto 93); che la necessità presuppone un trattamento "*oggettivamente indispensabile*" per realizzare una finalità che è parte integrante della prestazione destinata all'interessato, e che il titolare deve poter dimostrare in che modo l'oggetto principale del contratto non potrebbe essere conseguito senza il trattamento (punto 98); che la circostanza che il trattamento sia "*soltanto utile*" è irrilevante e occorre che "*non esistano altre soluzioni percorribili e meno invasive*" (punto 99); e che, se il contratto comprende più elementi distinti di uno stesso servizio, la valutazione va svolta separatamente per ciascuno (punto 100). Richiamati in via di analogia, tali criteri escludono che un accesso generale all'archivio possa dirsi strettamente necessario per un caricamento che può essere reso più "*efficiente*", ma è realizzabile con strumenti meno invasivi; e l'onere di dimostrare il contrario grava su Meta, che non vi ha provveduto.

Le basi giuridiche invocate da Meta. Quanto alle basi giuridiche invocate, l'Autorità condivide l'assunto di Meta secondo cui l'art. 122 del Codice e l'art. 6 del Regolamento operano su piani distinti. Ne discende che l'accesso alle informazioni archiviate nel terminale non può essere giustificato dal legittimo interesse né, al di fuori della stretta necessità, dalla necessità contrattuale, quali che siano le basi che Meta intende indicare per il trattamento successivo. Contrariamente a quanto Meta sostiene, l'atto di avvio non ha confuso i due piani: ha rilevato che, rispondendo alla richiesta dell'Autorità sulla base giuridica e sul meccanismo di consenso (quesiti 3 e 4 della richiesta del 27 ottobre 2025), Meta aveva indicato il contratto e il legittimo interesse, che non sono idonei a legittimare l'accesso ai sensi dell'art. 122. Con la memoria Meta chiarisce che per l'accesso fa valere il solo consenso espresso con l'autorizzazione di sistema e, in subordine, la stretta necessità: entrambi i fondamenti sono stati esclusi.

La distinzione tra i due piani, e le sue conseguenze, trovano riscontro nel parere 5/2019 dell'EDPB. Poiché l'art. 5, par. 3, della direttiva prevede come regola il consenso preliminare, esso, nella misura in cui le informazioni archiviate nel terminale costituiscono dati personali, "*prevale sull'articolo 6 del regolamento generale sulla protezione dei dati con riguardo alle attività di archiviazione di o accesso a tali informazioni*", e il titolare "*non può fare affidamento sull'intera gamma di condizioni di liceità di cui all'articolo 6*" (parere 5/2019, par. 40). Il contratto e il legittimo interesse indicati da Meta non possono dunque giustificare l'accesso legato alla Funzionalità. Essi possono venire in rilievo, semmai, per i trattamenti anteriori e successivi, che non sono disciplinati da una norma speciale della direttiva e restano di competenza dell'autorità capofila (parere 5/2019, par. 75), e che il presente provvedimento non esamina. Nello stesso senso, la Corte di giustizia ha ritenuto rilevante l'esame dell'art. 7, lett. f), della direttiva 95/46 solo perché i

dati trasmessi "*non si limitano necessariamente a informazioni archiviate nell'apparecchiatura terminale*" (Fashion ID, punto 91).

La scelta delle basi giuridiche in ragione dell'età. L'Autorità non si pronuncia sul rilievo, formulato nell'atto di avvio, secondo cui il ricorso a due basi giuridiche diverse in ragione dell'età dell'utente rifletterebbe una "scelta di convenienza", che attiene ai trattamenti disciplinati dal Regolamento e alla competenza dell'autorità capofila (par. 3.4). Non può però non osservare che tale scelta si pone nel solco delle soluzioni formalistiche e prive di reale consistenza giuridica che restituiscono un quadro contraddittorio e intrinsecamente debole delle scelte di fondo operate dal titolare rispetto ai trattamenti in esame.

3.7. L'informazione agli utenti (art. 122, comma 1, del Codice)

Sotto tale profilo, l'art. 122, comma 1, richiede che l'utente sia informato prima di esprimere il consenso. L'informazione resa da Meta è carente sotto quattro profili.

Gli utenti già attivi. Al riguardo, l'atto di avvio del procedimento ha rilevato che gli utenti già attivi al momento dell'introduzione della Funzionalità non hanno ricevuto alcuna informativa. Meta non lo contesta: si limita a osservare che "*non era richiesta una notifica aggiuntiva e separata*" (memoria, §5.31) e a indicare, quali strumenti di trasparenza (§5.32), l'informativa generale sulla privacy, l'avviso che precede la richiesta di autorizzazione e il suggerimento di condivisione. Si tratta, tuttavia, di strumenti che non raggiungono gli utenti che avevano già concesso l'autorizzazione prima del 2023. L'avviso, infatti, viene mostrato soltanto a chi l'autorizzazione non l'ha ancora concessa. Il suggerimento di condivisione compare quando la Funzionalità è già operativa e il trattamento già in corso, sicché non può per definizione costituire un'informazione preventiva. L'informativa generale, infine, è un documento che l'utente non può essere tenuto a riesaminare dopo ogni aggiornamento dell'app, e che, come già osservato, non descrive in modo specifico la Funzionalità. Né può valere a giustificare l'omissione l'argomento secondo cui i dati sarebbero "*non sensibili*" e il trattamento "*coerente con le funzionalità principali dell'App*" (§5.30): l'informazione preventiva è condizione di validità del consenso, che spetta a Meta dimostrare di aver dato agli utenti, a prescindere dalla natura dei dati trattati e dalla maggiore o minore prevedibilità del trattamento per l'utente medesimo.

La formula dell'informativa sulla privacy. Va inoltre osservato che la formula che Meta indica come riferimento alla Funzionalità ("*ricordarti quando hai nuove foto da caricare*") non identifica la Funzionalità e non ne descrive il funzionamento: essa non spiega che l'app seleziona autonomamente contenuti dalla galleria per proporre all'utente di pubblicarli. Tale formulazione, che Meta stessa dichiara inclusa nell'informativa sulla privacy dal luglio 2022 (memoria, §5.37), è anteriore al lancio della Funzionalità, avvenuto nel 2023 secondo Meta (nota del 14 novembre 2025): l'informativa non è stata dunque aggiornata in occasione del lancio. L'atto di avvio ha inoltre rilevato che l'informativa non contiene indicazioni specifiche sulla Funzionalità, e che la dicitura più vicina ("*Contenuti che fornisci tramite le nostre funzioni per la fotocamera, le tue impostazioni della galleria o le funzioni vocali*") ricorre ventitré volte nel testo, anche in connessione con finalità, come la personalizzazione delle inserzioni, che non emergono dalle informazioni fornite nel prodotto; su tale rilievo la memoria non formula alcuna replica. Meta richiama le Linee guida sulla trasparenza del Gruppo di lavoro Articolo 29, secondo cui il titolare deve bilanciare completezza e concisione. L'Autorità non ritiene che l'informativa debba descrivere ogni funzione di un'app, ma che le informazioni necessarie per decidere se consentire un trattamento particolarmente invasivo (la lettura dell'archivio fotografico dell'utente evidentemente lo è) vadano rese al momento in cui l'autorizzazione è richiesta, in modo specifico.

L'avviso che precede la richiesta di autorizzazione. L'avviso che precede la richiesta di autorizzazione indica, tra le finalità, quella di "*abilitare altre funzioni*": una formula generica, che non consente all'utente di comprendere a quali trattamenti stia effettivamente dando accesso. L'avviso, inoltre, non distingue tra la pubblicazione di singole foto, che richiede un accesso occasionale e limitato al contenuto scelto, e la Funzionalità, che presuppone invece un accesso ampio e continuativo all'intero archivio (ove l'utente scelga, come la richiesta di sistema induce a fare, l'opzione "Consenti tutto"). Né chiarisce che l'autorizzazione, una volta concessa, rende l'app in grado di leggere tutte le foto e i video presenti sul dispositivo e che essa resta valida per ogni funzione, non soltanto per quella per la quale è stata richiesta. Quanto alla schermata delle impostazioni, Meta ammette che l'opzione poteva apparire attiva ancor prima che l'autorizzazione fosse concessa (memoria, §4.33): in tal modo l'utente era posto di fronte a un'indicazione che non rifletteva la

situazione effettiva. L'Autorità prende atto delle modifiche introdotte con la versione 581 dell'app, dell'articolo del Centro Assistenza pubblicato nell'aprile 2026 e degli ulteriori aggiornamenti annunciati. Si tratta, tuttavia, di interventi successivi alla segnalazione (luglio 2025) e alla richiesta di informazioni dell'Autorità (ottobre 2025), che riguardano soltanto gli utenti che aggiornano l'app e che non possono sanare l'illiceità di un accesso avvenuto in precedenza. L'Autorità ne tiene conto esclusivamente ai fini della quantificazione della sanzione (par. 6.2).

Il contenuto dell'informazione dovuta. Quanto al contenuto dell'informazione dovuta, la Corte ha precisato che un'informazione "*chiara e completa*" implica che l'utente sia in grado di "*determinare agevolmente le conseguenze di un eventuale consenso prestato*" e di esprimerlo "*con piena conoscenza di causa*", e che le informazioni debbano essere "*chiaramente comprensibili e sufficientemente dettagliate*" (Planet49, punto 74; v. anche Orange România, punti 40 e 52, secondo cui l'informazione deve essere previa, in forma comprensibile e facilmente accessibile e con linguaggio semplice e chiaro). Nella stessa sentenza la Corte ha ricompreso nell'informazione dovuta la durata dell'attività dei cookie, perché un periodo lungo o illimitato implica la raccolta di numerose informazioni (Planet49, punti 75 e 78), nonché la possibilità di accesso da parte di terzi (punti 75 e 80). Per analogia, la permanenza dell'accesso concesso con l'autorizzazione di sistema, la sua estensione all'intero archivio (nella forma "Consenti tutto") e la sua validità per funzioni diverse da quella per cui è richiesta, sono informazioni essenziali per valutare le conseguenze della scelta e sono proprio quelle di cui l'avviso di Meta è privo. Il rilievo non muta se l'utente può scegliere un accesso limitato: neppure in tal caso l'avviso rende comprensibili la permanenza dell'accesso e la sua validità per ogni funzione dell'app, e la limitatezza dell'accesso non fa differenza ai fini del difetto di informazione. Quanto al momento dell'informazione, che deve essere immediata (Fashion ID, punto 104, già richiamato al par. 3.5), essa non può essere rinviata a documenti generali o a momenti successivi. Le Linee guida 5/2020 indicano, quali informazioni minime per un consenso informato, l'identità del titolare, la finalità di ciascuno dei trattamenti per i quali è richiesto il consenso e i tipi di dati che saranno raccolti e utilizzati (par. 64), da fornire in modo specifico per ciascuna richiesta di consenso distinta (par. 61), requisiti che l'avviso di Meta, riferito genericamente all'"abilitare altre funzioni", non soddisfa.

Nel complesso, l'utente non è stato posto in condizione di comprendere, prima di concedere l'accesso, che avrebbe abilitato Meta a una lettura sistematica dell'archivio fotografico per proporre contenuti da pubblicare. L'informazione non rispetta quindi il requisito dell'art. 122, comma 1, che l'utente sia informato "*con metodologie che assicurino l'effettiva consapevolezza*".

3.8. Ulteriori profili e dimensione del perimetro soggettivo della violazione

Per completezza e per rispondere alle deduzioni della Società, l'Autorità precisa che la responsabilità di Meta non si desume dai seguenti profili, pur emersi nell'istruttoria:

- la Relazione tecnica, e di conseguenza l'atto di avvio, si limitano ad affermare che la complessità delle schermate di impostazioni "*potrebbe costituire*" un ostacolo e che alcuni elementi "*potrebbero costituire*" modelli di progettazione ingannevoli ai sensi delle Linee guida 3/2022 dell'EDPB. Meta rileva che tali formulazioni sono cautelative (memoria, §5.45). L'Autorità non ne trae pertanto un addebito autonomo e li considera, nei limiti sopra indicati, solo quale contesto dell'inadeguatezza dell'informazione;

- la denominazione della Funzionalità**,** che le diverse formulazioni utilizzate nell'app ("*suggerimenti da condividere provenienti dalla galleria*", "*ottieni suggerimenti dalla galleria quando navighi su Facebook*", "*suggerimenti sulle foto da caricare*") potrebbero rendere equivoca; il rilievo, formulato in termini ipotetici, non è posto a fondamento della decisione;

- l'autorizzazione ACCESS_MEDIA_LOCATION risulta dichiarata nel Manifest e, secondo la Relazione tecnica, è "molto probabile" che sia accordata con la stessa finestra di sistema delle autorizzazioni sulle foto, pur non essendo possibile verificarlo. Meta dichiara che la Funzionalità non la utilizza e che essa è dichiarata a livello di applicazione per altre funzioni (memoria, §5.34-5.36). L'Autorità non accerta che la Funzionalità acceda a dati di ubicazione, ma prende atto che Meta riconosce che la medesima richiesta di autorizzazione copre funzioni diverse da quella in esame;

- l'impiego dei contenuti per l'addestramento dell'intelligenza artificiale, che Meta ha negato per i contenuti non pubblicati e che l'Autorità non è in grado di verificare, in assenza del codice dell'app e a

causa della cifratura del traffico, sicché la verifica avrebbe richiesto la più ampia collaborazione del titolare. Meta ha dichiarato, nel riscontro del 14 novembre 2025, che la Funzionalità non utilizza intelligenza artificiale generativa e che non intende utilizzare i contenuti non pubblicati della galleria per sviluppare e migliorare la propria IA, la quale sarebbe alimentata solo dai contenuti che l'utente adulto renda pubblici o condivida con Meta AI nell'ambito di un prompt, salvo opposizione. Nella memoria (§2.2) ha ribadito che la Funzionalità non implica IA generativa né trattamenti in cloud e non comporta analisi del contenuto di foto o video. Nella medesima memoria, tuttavia, in una nota (nota 4, al §1.3.6), la Società ha precisato che la stessa pagina delle impostazioni contiene un'ulteriore e distinta funzionalità, denominata "Ottieni idee creative su misura per te consentendo l'elaborazione nel cloud della galleria fotografica", presentata come "Novità", lanciata nell'Unione europea all'inizio del 2026 a seguito di una consultazione con la DPC, che non è oggetto del presente procedimento. La circostanza solleva interrogativi che l'Autorità non può risolvere allo stato degli atti: la nuova funzionalità, per sua stessa denominazione, comporta l'elaborazione nel cloud di Meta di contenuti della galleria, ossia ciò che per la Funzionalità in esame Meta esclude; poiché, secondo la stessa Società, l'autorizzazione di sistema operativo si applica all'app nel suo complesso (memoria, §6.1-6.3), essa potrebbe fondarsi sull'autorizzazione già accordata dagli utenti; non è chiaro se e con quali modalità gli utenti ne siano informati e vi consentano; e la smentita di Meta sull'addestramento è limitata ai contenuti "non pubblicati" ed è formulata in termini prospettici ("non intende"), sicché non chiarisce se i contenuti elaborati nel cloud, o i loro derivati, siano o possano essere riutilizzati per sviluppare e migliorare l'IA. Tali profili non sono posti a fondamento del presente provvedimento, ma l'Autorità si riserva di svolgere distinti accertamenti sulla nuova funzionalità, anche mediante richieste di informazioni (art. 157 del Codice) e accessi, ispezioni e verifiche (art. 158 del Codice), con riguardo alla base giuridica, all'informazione e al consenso degli utenti, al riutilizzo dei contenuti per l'addestramento dei modelli e al rapporto con l'autorizzazione di sistema già concessa, nonché di valutare il coordinamento con la DPC per i profili di rispettiva competenza. L'art. 122 non richiede, ai fini dell'illiceità accertata, tale verifica.

La dimensione del perimetro. Quanto alla dimensione del perimetro, Meta contesta la stima di circa 20 milioni di utenti, senza tuttavia fornire alcuna cifra alternativa, benché con l'atto di avvio le fosse stato richiesto di indicare ogni elemento utile ai fini dell'art. 83, par. 2, del Regolamento. Come già per l'architettura di sistema dell'app, anche con riguardo al bacino di estensione della Funzionalità Meta non ha ritenuto di dover fornire alcun chiarimento, pur essendo il solo soggetto in grado di conoscere il dato (il numero di utenti italiani su dispositivi Android che hanno concesso l'autorizzazione di sistema operativo). Ciò che Meta avrebbe dovuto fornire, in un'ottica di leale collaborazione con l'Autorità, è stato dunque ricostruito dall'Autorità stessa sulla base di fonti pubbliche e attendibili. Secondo l'Osservatorio sulle comunicazioni n. 4/2025 dell'AGCOM (par. 2.15, p. 28), elaborato su dati Audicom - Audiweb, nel settembre 2025 gli utenti unici mensili di Facebook in Italia erano 35,6 milioni. Secondo le rilevazioni basate sulle risorse pubblicitarie di Meta, riportate da DataReportal (Digital 2026: Italy), a fine 2025 il pubblico di Facebook in Italia era di circa 28,5 milioni di utenti. Considerato che, secondo le rilevazioni di Statcounter, il sistema Android rappresenta circa il 63% dell'uso mobile in Italia, ne risulta, applicando tale quota ai due dati, una platea compresa tra circa 18 e 22 milioni di utenti, che conferma la stima di circa 20 milioni contenuta nell'atto di avvio. Va peraltro rilevato che il numero esatto non è un elemento costitutivo della violazione e non incide sull'accertamento; quanto alla sanzione, l'Autorità ne tiene conto nei limiti dell'incertezza, che deriva dalla mancata collaborazione della Società e non può quindi operare a suo favore.

3.9. Elemento soggettivo

La violazione è stata commessa con significativa negligenza. Meta, infatti, è un operatore di dimensioni globali, che dispone di strutture specializzate in materia di conformità e che conosce il funzionamento del modello di autorizzazioni di Android e le politiche dei competitor per l'accesso a foto e video, le quali prevedono richieste incrementali, nel contesto, e nuovi consensi per scopi ulteriori. In particolare, la scelta di unire in un'unica richiesta funzioni con esigenze di accesso diverse, preimpostando come attiva la Funzionalità, è una scelta di progettazione della Società e non una conseguenza ineludibile del sistema operativo, come la Relazione tecnica ha dimostrato. La Società ha inoltre fornito all'Autorità, nella risposta del 14 novembre 2025, un'indicazione inesatta sullo stato dell'impostazione per gli utenti che non avevano concesso l'autorizzazione, rettificata soltanto con la memoria difensiva. Le misure successive non escludono la colpa e sono valutate ai fini della sanzione (par. 6.2)

4. CONCLUSIONI

Alla luce di tali considerazioni, risultano confermati i profili oggetto di contestazione con l'atto di avvio del procedimento di cui all'art. 166 del Codice, nei limiti precisati ai parr. 3.4 e 3.8, in quanto le dichiarazioni rese e la documentazione prodotta nel corso dell'istruttoria non sono idonee a superare i rilievi formulati dall'Ufficio e non ricorre alcuno dei casi previsti dall'art. 11 del regolamento n. 1/2019.

Pertanto, l'Autorità rileva l'illiceità della condotta posta in essere da Meta Platforms Ireland Limited, per aver effettuato, attraverso l'app Facebook per dispositivi Android, l'accesso a informazioni archiviate nei terminali degli utenti italiani (fotografie, video e relativi metadati) per la Funzionalità "Ottieni suggerimenti dalla galleria quando navighi su Facebook", senza aver acquisito un consenso specifico e informato per tale Funzionalità, distinto da quello relativo alle altre funzionalità dell'app, e senza aver informato preventivamente gli utenti con modalità idonee ad assicurarne l'effettiva consapevolezza, in violazione dell'art. 122, commi 1 e 2, del Codice. Non sono accertate violazioni autonome degli artt. 6, 7, 12 e 13 del Regolamento, richiamati quali parametri sostanziali nei termini di cui al par. 3.4.

Deve inoltre rilevarsi che la violazione accertata nei termini di cui in motivazione non può in alcun modo essere considerata "minore", tenuto conto del numero di interessati potenzialmente coinvolti (circa 20 milioni di utenti Android in Italia), della durata (dal 2023, secondo quanto dichiarato da Meta, e tuttora in corso per gli utenti che non hanno aggiornato l'app), della natura strutturale della scelta di progettazione e delle dimensioni e della capacità economica del titolare (v. considerando 148 del Regolamento).

5. MISURE CORRETTIVE

Va anzitutto rilevato che la condotta non risulta esaurita. Le modifiche introdotte con la versione 581 dell'app, secondo quanto dichiarato da Meta, riguardano soltanto gli utenti che aggiornano l'app; gli altri continuano a visualizzare la precedente interfaccia (memoria, nota 7), né Meta ha dichiarato di aver richiesto un nuovo consenso agli utenti italiani che avevano già concesso l'autorizzazione di sistema. La regolarizzazione dichiarata (articolo del Centro Assistenza, versione 581, aggiornamenti in preparazione) non è verificabile e non riguarda il meccanismo di acquisizione del consenso, né è corredata dei riscontri tecnici che l'Autorità, per sistemi di questo tipo, può ottenere solo dalla collaborazione del titolare (v. infra, par. 6.2). Appare quindi necessario impartire a Meta le misure correttive seguenti, proporzionate alle dimensioni e alla capacità tecnica della Società:

- ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, ingiunge a Meta di conformare i trattamenti, entro sessanta giorni dalla notifica, adottando le seguenti misure nei confronti degli utenti italiani di Facebook su dispositivi Android: (i) acquisire il consenso all'accesso alla galleria per la Funzionalità con una richiesta distinta e specifica, non accorpata alla richiesta di autorizzazione per la pubblicazione di foto e video né ad altre funzioni, e senza formule generiche come "*abilitare altre funzioni*"; (ii) informare l'utente, al momento della richiesta, in modo chiaro e comprensibile, sullo scopo della Funzionalità, sul fatto che essa comporta l'accesso all'archivio multimediale e sulle modalità per disattivarla e per revocare l'autorizzazione; (iii) mantenere la Funzionalità disattivata per impostazione predefinita e attivarla soltanto in seguito alla manifestazione di volontà dell'utente riferita ad essa; (iv) acquisire il consenso con tale modalità anche dagli utenti che hanno già concesso l'autorizzazione di sistema, tenendo disattivata la Funzionalità fino alla manifestazione di volontà; (v) assicurare che lo stato dell'impostazione corrisponda a quello effettivo del trattamento, per tutte le versioni dell'app in uso in Italia, anche con controlli lato server o con aggiornamenti obbligatori;

- ai sensi dell'art. 58, par. 2, lett. f), del Regolamento, vieta a Meta, decorso inutilmente il termine di sessanta giorni di cui al punto precedente, di rendere operativa la Funzionalità nei confronti degli utenti italiani di Facebook su dispositivi Android che non abbiano manifestato il consenso secondo le modalità indicate, fino all'adeguamento; vieta altresì a Meta il trattamento di qualunque informazione trattata mediante la Funzionalità in assenza del consenso acquisito secondo le modalità indicate;

- ai sensi dell'art. 58, par. 1, lett. a), del Regolamento e dell'art. 157 del Codice, ingiunge a Meta di comunicare all'Autorità entro trenta giorni le iniziative avviate, anche al fine della definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, nonché, entro novanta giorni dalla notifica, le soluzioni adottate per dare attuazione alle misure sopra indicate, allegando la relativa documentazione tecnica (anche schermate delle nuove interfacce e dichiarazioni sul funzionamento del trattamento, che

indichino se le informazioni della galleria, anche derivate, sono trasmesse ai sistemi di Meta prima della pubblicazione), nonché il numero di utenti italiani su dispositivi Android che hanno prestato il consenso con le nuove modalità.

6. ORDINANZA-INGIUNZIONE

Ai sensi degli artt. 58, par. 2, lett. i) del Regolamento e dell'art. 166 del Codice, il Garante ha il potere di infliggere una sanzione amministrativa pecuniaria ai sensi dell'art. 83 del Regolamento, mediante l'adozione di una ordinanza ingiunzione (v. artt. 18, l. 24 novembre 1981, n. 689 e 16, comma 1, del regolamento del Garante n. 1/2019).

6.1. Valutazione della condotta e individuazione della sanzione applicabile

La violazione dell'art. 122 del Codice è soggetta alla sanzione prevista dall'art. 83, par. 5, del Regolamento, in forza dell'art. 166, comma 2, del Codice. Poiché è accertata la violazione di un'unica disposizione, in conseguenza di un'unica condotta (la progettazione e l'operatività della Funzionalità con il meccanismo di accesso descritto), non trova applicazione l'art. 83, par. 3, del Regolamento.

Ai fini della quantificazione occorre anzitutto individuare il limite massimo edittale, che è pari a 20 milioni di euro o, se superiore, al 4% del fatturato mondiale totale annuo dell'esercizio precedente (art. 83, par. 5, del Regolamento). Al riguardo, il massimale dinamico prevale su quello statico quando il fatturato dell'impresa supera i 500 milioni di euro (Comitato europeo per la protezione dei dati, "Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR", versione 2.1 adottata il 24 maggio 2023, di seguito "Linee guida 4/2022", par. 114-116).

La nozione di impresa. Al riguardo, si deve rappresentare che il parametro non è il fatturato della sola società destinataria del provvedimento. Infatti, l'art. 83, parr. 4-6, del Regolamento, alla luce del considerando 150, rinvia alla nozione di "impresa" degli artt. 101 e 102 TFUE, che designa un'unità economica anche se costituita da più persone giuridiche: quando il titolare del trattamento fa parte di un'impresa così intesa, il limite massimo dinamico si calcola sul fatturato dell'impresa nel suo complesso (Linee guida 4/2022, par. 118-122; Corte di giustizia, sentenza del 5 dicembre 2023, C-807/21, Deutsche Wohnen, punti 53-59). Sotto altro profilo, se la società madre detiene la totalità o quasi del capitale della controllata, si presume che eserciti su di essa un'influenza determinante, salvo prova contraria (c.d. presunzione Akzo; Corte di giustizia, sentenza del 10 settembre 2009, C-97/08 P, Akzo Nobel, punti 60-61; Linee guida 4/2022, par. 124-125). Nel caso di specie, Meta Platforms Ireland Limited ha prodotto il proprio bilancio d'esercizio al 31 dicembre 2024, certificato il 30 luglio 2025, dal quale risulta che la propria ultima società controllante è Meta Platforms, Inc. Dai registri del progetto Media Ownership Ireland (iniziativa di Coimisiún na Meán e della DCU School of Communications; dati aggiornati a dicembre 2025, consultati il 25 ottobre 2026 e acquisiti agli atti) risulta inoltre una catena di controllo interamente totalitaria: Meta Platforms Ireland Limited (n. 462932) è detenuta al 100% da Facebook International Operations Limited (n. 514293), a sua volta detenuta al 100% da Facebook Ireland Holdings Unlimited Company (n. 466405), il cui capitale è interamente detenuto da Meta Platforms, Inc. Il Form 10-K di Meta Platforms, Inc. per gli esercizi chiusi al 31 dicembre 2024 e 2025, depositato presso la Securities and Exchange Commission (all. 21.1, elenco delle società controllate), include Meta Platforms Ireland Limited tra le controllate di Meta Platforms, Inc., coerentemente con quanto risulta dal bilancio d'esercizio prodotto. L'elenco non reca alcuna indicazione di una partecipazione inferiore alla totalità del capitale della società né di altri soci, e conferma dunque, in assenza di diversa specificazione, il quadro di controllo totalitario emergente dai registri sopra richiamati. La partecipazione totalitaria lungo l'intera catena, che fa capo a Meta Platforms, Inc., fa dunque operare la presunzione di influenza determinante esercitata dalla società madre, e Meta non ha addotto elementi idonei a superarla. L'impresa di riferimento è pertanto il gruppo che fa capo a Meta Platforms, Inc., il cui fatturato si desume dal bilancio consolidato (Linee guida 4/2022, par. 128-130).

I dati economici di riferimento. Quanto ai dati economici di riferimento, il bilancio consolidato di Meta Platforms, Inc. (Form 10-K, accession n. 0001628280-26-003942, Item 8, "Consolidated Statements of Income") per l'esercizio chiuso al 31 dicembre 2025, ultimo esercizio chiuso e pubblico alla data della presente decisione, espone ricavi per 200.966 milioni di dollari statunitensi e un utile netto di 60.458 milioni di dollari. Occorre peraltro considerare che il fatturato rilevante è quello dell'esercizio che precede la decisione con cui è irrogata la sanzione (Linee guida 4/2022, par. 131). Ciò posto, applicando il tasso di cambio di riferimento pubblicato dalla Banca centrale europea per il 31 dicembre 2025, data di chiusura

dell'esercizio (1 euro = 1,1750 dollari statunitensi; Gazzetta ufficiale dell'Unione europea, serie C, C/2026/44 del 5 gennaio 2026), il fatturato è pari a circa 171.035 milioni di euro (euro 171.034.893.617) e l'utile netto a circa 51.454 milioni di euro. Il massimale dinamico, pari al 4% del fatturato, è dunque di circa 6.841 milioni di euro (euro 6.841.395.745), largamente superiore al massimale statico di 20 milioni di euro, che non rileva.

Va infine precisato che il massimale non è commisurato al fatturato realizzato in Italia né al perimetro della contestazione: il Regolamento lo collega alla dimensione economica dell'impresa nel suo insieme, mentre il carattere nazionale della violazione e il numero di utenti coinvolti rilevano ai fini della gravità (par. 6.2).

6.2. Quantificazione della sanzione amministrativa pecuniaria (art. 83, par. 2, del Regolamento)

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

A tal fine, l'Autorità segue, a fini di trasparenza e uniformità, la metodologia indicata dall'EDPB nelle Linee guida 4/2022, che si articola nell'individuazione del punto di partenza (classificazione della violazione, gravità, fatturato dell'impresa), nella valutazione delle circostanze aggravanti e attenuanti e nella verifica finale di effettività, proporzionalità e dissuasività, senza che ciò comporti un calcolo meramente aritmetico, che deve sempre fondarsi su una valutazione di tutte le circostanze del caso (par. 145). Inoltre, ciascun criterio dell'art. 83, par. 2, è considerato una sola volta (par. 72 e 133) e la dimensione dell'impresa non è computata due volte (par. 64).

Gravità della violazione. Ai fini della quantificazione, il punto di partenza è la gravità della violazione nel caso concreto, valutata alla luce della natura, gravità e durata della violazione (art. 83, par. 2, lett. a)), del carattere doloso o colposo (lett. b)) e delle categorie di dati interessate (lett. g)), considerati nel loro complesso (Linee guida 4/2022, par. 51-52 e 59). La violazione rientra anzitutto tra quelle per le quali l'art. 83, par. 5, prevede il massimale più elevato, che esprime la maggiore gravità in astratto (par. 49-50). Nel caso concreto rilevano i seguenti elementi:

- natura della violazione: l'art. 122 tutela l'integrità della sfera privata dell'utente e la sua autodeterminazione rispetto all'accesso al terminale; la violazione ha riguardato il presupposto stesso di tale tutela, cioè un consenso preventivo, specifico e informato, mai richiesto per la Funzionalità, sicché l'obiettivo della disposizione è stato frustrato nella sostanza (Linee guida 4/2022, par. 53, lett. a)). Il contesto è quello di un trattamento di natura commerciale svolto da un operatore in posizione di forte asimmetria informativa rispetto agli utenti, mediante un sistema chiuso e non verificabile, rispetto al quale l'Autorità necessita della più ampia collaborazione del titolare (v. par. 3.3), su un archivio che può contenere immagini di minori o comunque sensibili, la cui presenza è potenziale e non accertata (par. 53, lett. b), i));

- oggetto del trattamento e numero di interessati: la violazione ha portata nazionale e riguarda l'archivio multimediale degli utenti che abbiano concesso l'autorizzazione, in forma completa o limitata, attraverso un'app di uso quotidiano; la platea coinvolta è nell'ordine di venti milioni di utenti Android in Italia secondo la stima in atti, che Meta non ha smentito con dati propri benché richiesti, e rappresenta una quota considerevole della popolazione residente; il numero comprende anche utenti che non hanno mai utilizzato la Funzionalità, e ciò conferisce alla violazione un carattere sistemico (par. 53, lett. b), ii) e iv));

- finalità del trattamento: la Funzionalità è diretta ad aumentare l'uso e la condivisione di contenuti sulla piattaforma, attività centrale dell'impresa; quanto più il trattamento è centrale rispetto alle attività principali del titolare, tanto più gravi sono le irregolarità (par. 53, lett. b), iii)). L'elemento è valutato in questa sede e non è computato nuovamente come circostanza ai sensi dell'art. 83, par. 2, lett. k);

- durata: secondo Meta la Funzionalità è stata introdotta nel 2023 e la condotta è tuttora in corso per gli utenti che non hanno aggiornato l'app e per quelli che hanno già concesso l'autorizzazione di sistema, sicché la violazione si è protratta per più anni (par. 53, lett. c));

- livello del danno: non risulta provato un pregiudizio concreto e individuale, e l'Autorità non ha accertato trasmissioni, usi ulteriori o trattamenti di categorie particolari di dati; rileva tuttavia il danno

potenziale, non marginale, della perdita di controllo dell'utente sull'accesso a un archivio di contenuti privati, che il Regolamento considera anche quando il danno "*potrebbe essere stato subito*" e non richiede di provare ai fini della sanzione (par. 53, lett. b), v)). In tal senso, la Corte di giustizia ha riconosciuto, pur nel diverso contesto della ponderazione ex art. 6, par. 1, lett. f), del Regolamento, che un trattamento molto esteso e incidente in modo rilevante sull'utente "*può suscitare in quest'ultimo la sensazione di una continua sorveglianza della sua vita privata*" (sentenza del 4 luglio 2023, C-252/21, Meta Platforms e a., punto 118; v. anche i punti 112 e 117 sulle ragionevoli aspettative dell'utente). Il fattore ha, in concreto, peso limitato;

− carattere doloso o colposo (art. 83, par. 2, lett. b)): la violazione è colposa, non essendo emersa un'intenzione di eludere la norma; la colpa non è tuttavia lieve, trattandosi di un operatore di dimensioni globali, pienamente consapevole delle regole e del modello di autorizzazioni del sistema operativo (v. par. 3.9), che avrebbe potuto evitare scelte di progettazione come la richiesta unica di autorizzazione per più funzioni, la preimpostazione della Funzionalità come attiva e un'informazione generica; colposo non equivale a non volontario e il grado di colpa può assumere rilievo (par. 55-56);

− categorie di dati (art. 83, par. 2, lett. g)): fotografie, video e metadati (data e ora, tipologia, orientamento) sono dati comuni e non è stato accertato l'uso di dati di ubicazione o di categorie particolari; l'autorizzazione, nella forma "Consenti tutto" che la richiesta di sistema induce a concedere, abilita tuttavia l'accesso all'intero archivio, e la quantità di dati relativi a ciascun interessato aggrava la lesione della riservatezza (par. 58), tanto più che l'archivio può contenere informazioni di natura particolarmente riservata (par. 57). Anche la Corte di giustizia ha rilevato che, per i dati idonei a rivelare categorie particolari di informazioni, il rischio per i diritti fondamentali sussiste "*a prescindere da quale sia la loro finalità dichiarata*" e dal fatto che il titolare agisca allo scopo di ottenerle (C-252/21, punti 69-70), senza che ciò costituisca presupposto dell'accertamento.

Considerati nel loro complesso, tali elementi (portata nazionale e sistemica, durata, centralità per l'attività principale, quantità di dati accessibili, grado non lieve di colpa), a fronte dell'assenza di un danno concreto accertato, di dolo, di trasmissioni accertate e di categorie particolari di dati, inducono a ritenere che il livello di gravità della violazione sia medio (Linee guida 4/2022, par. 60), nella parte bassa della fascia.

Importo iniziale. Ciò premesso, per la gravità media l'importo iniziale è compreso tra il 10% e il 20% del limite massimo applicabile (par. 60). A tale riguardo, poiché il fatturato dell'impresa supera ampiamente i 500 milioni di euro, non si applica alcun adeguamento dell'importo iniziale in funzione delle dimensioni, perché la dimensione dell'impresa è già riflessa nel massimale dinamico (par. 66, ultimo alinea). Applicando tale fascia al massimale di euro 6.841.395.745, l'importo iniziale è compreso tra circa 684,1 e circa 1.368,3 milioni di euro. Si osserva, inoltre, che le fasce non sono importi fissi e che l'Autorità può utilizzare l'intero intervallo, fino al massimale di legge, per adattare la sanzione alle circostanze del caso (par. 47 e 69). Alla luce degli elementi sopra valutati, in particolare dell'assenza di dolo, di danno concreto accertato, di trasmissioni accertate e di categorie particolari di dati, che compensano solo in parte gli elementi di segno opposto, l'importo iniziale è determinato nel 10,2% del massimale, pari a euro 700.000.000.

Quanto alle circostanze aggravanti e attenuanti (Linee guida 4/2022, cap. 5), ciascuna considerata una sola volta e senza ripetere i fattori già valutati ai fini della gravità (par. 72), si ritiene che debbano essere prese in considerazione le seguenti:

− Meta ha introdotto, dopo la segnalazione e la richiesta dell'Autorità, la versione 581 dell'app, con un'impostazione che non può essere attivata in assenza dell'autorizzazione di sistema, ha pubblicato nell'aprile 2026 un articolo del Centro Assistenza e ha annunciato ulteriori aggiornamenti; si tratta di una circostanza attenuante di peso moderato, perché tardiva, riferita solo agli utenti che aggiornano l'app e non incidente sul meccanismo di acquisizione del consenso né sugli utenti che avevano già concesso l'autorizzazione (cfr. art. 83, par. 2, lett. c), del Regolamento (Linee guida 4/2022, par. 75-76, secondo cui le misure attuate dopo l'avvio dell'indagine sono considerate diversamente, quali attenuanti, rispetto a quelle spontanee);

− Meta determina l'architettura dell'app e del meccanismo di richiesta delle autorizzazioni e ne ha il pieno controllo; non risulta che abbia adottato misure per separare la richiesta di accesso per la Funzionalità da quella per la pubblicazione (cfr. art. 83, par. 2, lett. d), del Regolamento; Linee guida

4/2022, par. 77 e 81). Il fattore ha un moderato effetto aggravante, atteso il maggiore livello di responsabilità previsto dal Regolamento (par. 81);

− Non si tiene conto, in assenza di accertamenti definitivi specifici su questa Funzionalità, delle procedure regolatorie pendenti cui si riferiscono le note al bilancio prodotto (cfr. art. 83, par. 2, lett. e), del Regolamento) e, quanto ai precedenti, rileva l'ordinanza ingiunzione del Garante del 14 giugno 2019, n. 134 (doc. web n. 9121486, di seguito "ordinanza n. 134/2019"), con la quale è stata irrogata a Facebook Ireland Ltd, oggi Meta Platforms Ireland Limited, in solido con Facebook Italy S.r.l., la sanzione di euro 1.000.000 ai sensi dell'art. 164-bis, comma 2, del Codice (nel testo previgente) per violazioni degli artt. 13 e 23 del Codice, in relazione alla comunicazione dei dati di 214.077 utenti italiani sulla base di un'informativa generica e di un consenso non specifico, con impostazioni preselezionate e senza alternative per l'utente. Si tratta di una violazione già accertata prima della presente decisione, commessa dal medesimo titolare, di oggetto affine e comunque realizzata con modalità analoghe (Linee guida 4/2022, par. 82 e 87-92). Il tempo trascorso e la diversa disciplina allora vigente ne riducono il peso (par. 84-86 e 91), senza escluderlo, non essendo previsti termini di estinzione (par. 85). Il fattore ha pertanto un lieve effetto aggravante (par. 94);

− Meta ha risposto alle richieste dell'Autorità, ha esercitato il diritto di accesso e ha prodotto una memoria articolata; il contegno complessivo non è tuttavia conforme al dovere di cooperazione che grava sul titolare del trattamento. La Società ha infatti presentato come "volontaria" una cooperazione che è invece dovuta per legge, e la cui falsità nelle dichiarazioni è sanzionata dall'art. 168 del Codice; ha fornito nella risposta del 14 novembre 2025 un'indicazione inesatta sullo stato dell'impostazione, rettificata solo con la memoria difensiva; non ha corredato le proprie dichiarazioni di alcun elemento tecnico che ne consentisse il riscontro, benché l'app Facebook sia un software chiuso, con traffico cifrato, rispetto al quale l'Autorità non può prescindere dalla più ampia collaborazione del titolare, il solo in grado di fornire i dati e gli elementi necessari a ricostruire il funzionamento effettivo della Funzionalità; e ha omesso di indicare il numero degli utenti che hanno concesso l'autorizzazione, nonché gli altri dati richiesti ai fini dell'art. 83, par. 2, così rendendo più gravosa la valutazione della portata della violazione. Un simile atteggiamento, che ha rimesso all'Autorità l'onere di ricostruire fatti rientranti nella esclusiva disponibilità della Società, non è improntato alla collaborazione richiesta a un operatore di tali dimensioni e consapevolezza, e non ha in alcun modo contribuito a limitare o evitare effetti negativi sui diritti degli utenti. Il grado di cooperazione deve pertanto ritenersi scarso e costituisce una circostanza aggravante di peso significativo (art. 83, par. 2, lett. f), del Regolamento; Linee guida 4/2022, par. 96-97;

− l'Autorità è venuta a conoscenza dei fatti tramite la segnalazione di un'associazione dei consumatori e non per iniziativa di Meta (cfr. art. 83, par. 2, lett. h), del Regolamento), fattore neutro, non essendo ravvisabile una notifica spontanea (Linee guida 4/2022, par. 98-99);

− la Funzionalità è diretta, secondo Meta, a favorire la condivisione di contenuti sulla piattaforma; l'attività di Meta Platforms Ireland Limited consiste, secondo le note al bilancio, nella fatturazione di prodotti pubblicitari su Facebook e sugli altri servizi del gruppo, sicché l'incremento dell'uso della piattaforma comporta un vantaggio economico, non quantificabile agli atti (cfr. art. 83, par. 2, lett. k), del Regolamento), e, in assenza di elementi sui profitti tratti dalla violazione, il fattore non è considerato aggravante (Linee guida 4/2022, par. 108-110);

− non risultano provvedimenti correttivi già disposti nei confronti di Meta sullo stesso oggetto né adesione a codici di condotta o a meccanismi di certificazione pertinenti (art. 83, par. 2, lett. i) e j), del Regolamento): fattori neutri.

Il bilanciamento delle circostanze. In sintesi, le circostanze sopra indicate, nel loro complesso, determinano un saldo aggravante. L'attenuante di cui alla lett. c), cui si attribuisce un peso moderato, è infatti superata dalle aggravanti di cui alle lett. d), per il grado di responsabilità, e), per la violazione precedente, e f), per la scarsa cooperazione; gli altri fattori sono neutri. Ne deriva un aumento dell'importo iniziale di 700 milioni di euro, già fissato nella parte bassa della fascia media, che viene pertanto determinato in 805 milioni di euro. Tale importo resta pienamente compreso nell'intervallo del 10-20% del massimale. Si conferma che le condizioni economiche dell'impresa non sono ulteriormente computate, perché già riflesse nel massimale dinamico utilizzato per determinare l'importo iniziale (par. 64 e 66).

Meta chiede, in via di estremo subordine, di limitare la risposta dell'Autorità a un richiamo non pubblico, adducendo l'assenza di danno, il carattere limitato dei dati e il carattere *de minimis* della violazione. Le circostanze indicate, già considerate, non consentono di qualificare la violazione come "minore" ai sensi del considerando 148 del Regolamento: il numero di utenti coinvolti, la durata, la natura strutturale della violazione e la persistenza di una parte della condotta impongono una sanzione pecuniaria, la quale, in quanto effettiva, proporzionata e dissuasiva (art. 83, par. 1), dev'essere commisurata alla dimensione dell'impresa, anche in considerazione del fatto che il massimale edittale non è riferito al solo perimetro nazionale. La qualificazione come violazione "minore" è del resto incompatibile con il livello di gravità medio e con la portata sistemica accertata (Linee guida 4/2022, par. 60).

Effettività, proporzionalità e dissuasività. L'importo così determinato è stato infine verificato alla luce dei requisiti dell'art. 83, par. 1, del Regolamento (Linee guida 4/2022, cap. 7). Sotto il profilo dell'effettività, l'importo è idoneo a sanzionare la condotta illecita e a rafforzare il rispetto della norma, anche in vista del ripristino della conformità disposto con le misure correttive (par. 135). Quanto alla proporzionalità, esso va commisurato sia alla gravità della violazione sia alle dimensioni dell'impresa (par. 139): l'importo che si ritiene di applicare corrisponde a circa lo 0,47% del fatturato mondiale e a circa l'1,56% dell'utile netto del gruppo per l'esercizio 2025, e al 11,7% del massimale di legge, dal quale resta ben distante; Meta non ha dedotto né documentato alcuna incapacità contributiva (par. 140-141). Sotto il profilo della dissuasività, l'importo non è assorbibile come mero costo dell'attività da parte di un'impresa di tali dimensioni, il che ne assicura la dissuasione specifica; esso indica inoltre agli operatori che l'uso di autorizzazioni generiche del sistema operativo per accedere ai contenuti degli utenti per finalità diverse è sanzionato in misura significativa, il che ne assicura la dissuasione generale (par. 142-143). Non si ritiene pertanto di applicare un coefficiente moltiplicatore di dissuasione (par. 144), né di ridurre l'importo.

In ragione dei suddetti elementi, valutati nel loro complesso, e in base ai principi di effettività, proporzionalità e dissuasività previsti dall'art. 83, par. 1, del Regolamento, si ritiene di determinare l'ammontare della sanzione pecuniaria nei confronti di Meta Platforms Ireland Limited nella misura di euro 805.000.000 (ottocentocinque milioni) per la violazione dell'art. 122, commi 1 e 2, del Codice.

6.3. Sanzione accessoria della pubblicazione

In conclusione, 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, si debba applicare a Meta la sanzione accessoria della pubblicazione del presente capo del provvedimento contenente l'ordinanza-ingiunzione sul sito internet del Garante, in ragione del particolare disvalore della condotta: un meccanismo di accesso alla galleria fotografica di un numero molto elevato di utenti (circa 20 milioni di utenti Android in Italia), impostato nel 2023 da un operatore di dimensioni globali con una richiesta di autorizzazione unica per più funzioni, con la Funzionalità preimpostata come attiva e con un'informazione agli utenti insufficiente per assicurarne l'effettiva consapevolezza, ancora in corso per una parte degli stessi.

PER QUESTI MOTIVI

ai sensi degli artt. 57 e 83 del Regolamento, si dichiara l'illiceità del trattamento di dati personali effettuato da Meta Platforms Ireland Limited, con sede legale in Merrion Road, Dublin 4, D04 X2K5 (Irlanda), numero di registrazione IE462932, con domicilio eletto ai fini del presente procedimento presso gli avv.ti XX e XX, XX, per la violazione dell'art. 122, commi 1 e 2, del Codice, nei termini di cui in motivazione;

ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, si prescrive a Meta Platforms Ireland Limited di conformarsi, entro il termine di sessanta giorni dalla data della notifica del presente provvedimento, alle prescrizioni formulate nel par. 5, primo punto, del presente provvedimento;

ai sensi dell'art. 58, par. 2, lett. f), del Regolamento, si vieta a Meta Platforms Ireland Limited, decorso inutilmente il termine di cui al punto precedente, di rendere operativa la Funzionalità nei confronti degli utenti italiani di Facebook su dispositivi Android che non abbiano manifestato il consenso con le modalità indicate nel par. 5, primo punto, del presente provvedimento; si vieta altresì a Meta Platforms Ireland Limited il trattamento di qualunque informazione trattata mediante la Funzionalità in assenza del consenso acquisito secondo le modalità indicate;

ai sensi dell'art. 58, par. 1, lett. a), del Regolamento e dell'art. 157 del Codice, si ingiunge a Meta Platforms Ireland Limited di comunicare all'Autorità, entro trenta giorni, le iniziative avviate, anche al fine della definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, nonché, entro il termine di novanta giorni dalla notifica del presente provvedimento, le iniziative intraprese al fine di dare attuazione alle misure imposte ai punti precedenti, nei termini indicati nel par. 5, terzo punto;

SI ORDINA

ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, a Meta Platforms Ireland Limited di pagare la somma di euro 805.000.000 (ottocentocinque milioni) a titolo di sanzione amministrativa pecuniaria per la violazione indicata in motivazione.

SI INGIUNGE

alla predetta società, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma sopra indicata, secondo le modalità indicate in allegato, entro 60 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dell'art. 27 della legge n. 689/1981.

Si rappresenta che, ai sensi dell'art. 166, comma 8, del Codice, resta salva la facoltà per il trasgressore di definire la controversia adeguandosi alle prescrizioni del Garante e 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. 1° settembre 2011, n. 150 previsto per la proposizione del ricorso come di seguito indicato;

SI DISPONE

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

Ai sensi dell'art. 78 del Regolamento, nonché degli artt. 152 del Codice e 10 del d.lgs. 1° settembre 2011, n. 150, avverso il presente provvedimento è possibile proporre opposizione all'autorità giudiziaria ordinaria, con ricorso depositato presso il tribunale ordinario del luogo individuato nel medesimo art. 10, a pena di inammissibilità, entro il termine di trenta giorni dalla data di comunicazione del provvedimento ovvero entra sessanta giorni se il ricorrente risiede all'estero.

Roma, 13 novembre 2026

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Montuori

ITALIAN DATA PROTECTION AUTHORITY

AT today's meeting, attended by Prof. Pasquale Stanzione, Chair; Prof. Ginevra Cerrina Feroni, Vice-Chair; Dr Agostino Ghiglia, Member; and Dr Luigi Montuori, Secretary-General;

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter the 'Regulation');

HAVING REGARD TO the Personal Data Protection Code (Legislative Decree No. 196 of 30 June 2003) (hereinafter the "Code");

HAVING REGARD TO Regulation No 1/2019 concerning internal procedures of external relevance, aimed at the performance of the tasks and the exercise of the powers conferred upon the Data Protection Authority, approved by Resolution No. 98 of 4 April 2019, published in the Official Gazette No. 106 of 8 May 2019 and at www.gpdp.it, web doc. No. 9107633 (hereinafter "Regulation No. 1/2019 of the Data Protection Authority");

HAVING REGARD TO the documentation on file;

HAVING REGARD TO the observations made by the Secretary-General pursuant to Article 15 of the Data Protection Authority Regulation No. 1/2000 on the organisation and functioning of the Office of the Data Protection Authority, adopted by resolution of 28 June 2000 (web doc. No. 1098801);

RAPPORTEUR: Prof. Pasquale Stanzione;

1. FACTS AND COURSE OF THE PRELIMINARY INVESTIGATION

1.1. Origin of the preliminary investigation

These proceedings stem from a complaint lodged on 10 July 2025 by the Bolzano Consumer and User Protection Centre (Verbraucherzentrale Südtirol, hereinafter 'CTCU') against the Irish company Meta Platforms Ireland Ltd (hereinafter 'Meta' or 'the Company' or 'the data controller').

The CTCU's complaint. According to the complaint, Meta, without prior notice, allegedly made a subtle change to the Facebook app used on its users' smartphones, and, consequently, to its relationship with them, by introducing a feature called 'Personalised sharing suggestions from your gallery', comprising two sub-options: one, through which Meta would access the metadata and content of the device's photo gallery (favourite videos, photo timestamps) to automatically generate pre-edited content (transitions, music, effects); the other, which would activate whilst the user is browsing Facebook, displaying images from their local gallery as suggestions for potential posts on the social network. The CTCU argued that users would not have been informed of the change nor would they have given valid consent, as this was an option with 'tacitly preset' consent, and suggested a link to the training of Meta's artificial intelligence systems.

The subject matter of the decision. This decision concerns the feature 'Get suggestions from your gallery whilst browsing Facebook' (hereinafter, the 'Feature'), accessible via the 'Suggestions to share from your gallery' settings page. The 'Personalised suggestions to share from your gallery' option is not the subject of these proceedings; Meta has stated that this option was never available in the European Region and was visible to some users due to a display error (a so-called 'bug'), nor the separate feature 'Get creative ideas tailored to you by enabling cloud processing of your photo gallery', which Meta reports was launched in the European Union in early 2026 and which the Notice of Initiation did not consider. The possible use of unpublished content for training artificial intelligence systems is not the subject of this investigation, due to a

lack of evidence, and Meta has denied carrying out such practices.

From a methodological perspective, it is necessary to first outline the characteristics of the Facebook app feature found on the settings page entitled ‘Sharing suggestions from your gallery’.

1.2. Key features of the feature

The Feature enables Meta to present the user, whilst browsing the Facebook platform, with basic sharing suggestions drawn from the gallery on their device.

For the feature to work, the option ‘Get suggestions from your gallery whilst browsing Facebook’ – found in the Facebook app settings – must be set to “on”, as also confirmed by Meta (“When a user grants device permission for their gallery, the activation option shown in Figure 1 for receiving basic sharing suggestions is set to ‘on’ (for clarity, the aforementioned Figure 1 is also reproduced below).

The Company has clarified that users can control the Feature at any time by using the dedicated button next to the text “Get suggestions from your gallery when browsing Facebook”.

1.3. Action taken

Request for information. By letter dated 27 October 2025 (ref. no. 142506), issued in the exercise of the powers conferred by Article 122 of the Code, the Office requested information and documents from Meta regarding the Feature:

the manner in which Italian users were informed prior to activation;
the technical functioning and scope of the processing;
the legal basis;
the interface and mechanism for obtaining consent, specifying whether the default setting was ‘active’ or ‘inactive’;
any further uses, including for the training of artificial intelligence models;
retention periods;
measures concerning special categories of data and images of minors;
and procedures for withdrawal of consent.

Meta’s response. In response to the Authority’s request for information, Meta first formally contested the Data Protection Authority’s competence to act directly, arguing that the processing in question falls under the exclusive jurisdiction of the Irish Data Protection Commission (hereinafter ‘DPC’), as the lead authority, pursuant to the one-stop-shop mechanism provided for in Article 56 of the Regulation. Furthermore, Meta considered the Data Protection Authority’s argument—that the Feature falls within the scope of the e-Privacy Directive (and therefore Article 122 of the Code) in the absence of ‘tracking tools’—to be unfounded.

Meta’s statements. Meta stated that the Feature has been available since 2023 and is not linked to generative artificial intelligence, challenging, as a preliminary matter, the Data Protection Authority’s jurisdiction in favour of the DPC, as well as the applicability of Article 122 of the Code, in the absence of ‘tracking tools’. Whilst stating that it provides the information ‘voluntarily’, Meta argued, in summary, that:

(i) access to the photo gallery requires authorisation at operating system level, which the user may grant either in full or limited to selected content;
(ii) the Feature processes the most recent photos and ‘basic metadata’ (date and time the photo was taken, photos marked as favourites, photo type or orientation), whilst there is no mention of the use of geolocation data or full EXIF data;
(iii) when the user grants device authorisation, the option ‘Get suggestions from your gallery whilst browsing Facebook’ is set to ‘on’, whilst for other users it is ‘off’ by default;
(iv) when the Feature is active, “Meta presents the user, whilst browsing Facebook, with basic sharing suggestions drawn from their gallery”;
(v) the legal basis is contractual necessity for users with full legal capacity and legitimate interest for minors;
(vi) the processing would take place entirely on the device and would not involve the processing of special categories of data;

(vii) transparency would be ensured by the privacy notice and the information provided within the product. Meta has also stated that it has forwarded a copy of the response to the DPC “as a courtesy”.

Technical assessment. On the basis of the statements made by Meta, the Office requested the Data Protection Authority’s Department of Digital Technologies and IT Security, by internal memo dated 2 December 2025 (ref. no. 168848), a technical assessment of the Feature, aimed at describing its main characteristics with regard to user consent and the processing of personal data, as well as the scope of application of Article 5(3) of Directive 2002/58/EC (‘the ePrivacy Directive’).

The findings of the Technical Report. The technical analysis, set out in note ref. no. 76045 of 18 May 2026 (hereinafter the “Technical Report”), was carried out by installing the Facebook app from scratch on an Android smartphone running the Android 14 operating system, thereby enabling the app’s behaviour to be observed under first-use conditions, and utilised technical tools such as the ‘Apk Analyzer’ and the Android Studio development environment to analyse the AndroidManifest.xml file (a configuration file that informs the operating system what the app is and what it is intended to do), extracted from the APK package of version 548.1.0.51.64 of the application, downloaded from a third-party website and verified for authenticity using the apksigner tool.

The following points emerged:

− on first launch, access to ‘Photos and videos’ is denied; the app can only access them once the user has granted the relevant operating system permissions via a single request covering both photos and videos, even though these are two distinct permissions (READ_MEDIA_IMAGES and READ_MEDIA_VIDEO);

− the option ‘Get suggestions from your gallery whilst browsing Facebook’ is preset as active, but, in the absence of operating system authorisation, it does not offer any suggestions: the feature cannot operate until the user grants the permissions;

− on the first attempt to create a post with a single photo, a story or a reel, the app displays a screen stating that access to the gallery is required to “share photos and videos, receive suggestions on which photos to upload and enable other features”, and directs the user to grant the broad READ_MEDIA permissions; the access granted is, as a rule, permanent and can only be revoked in the device’s settings;
− Android 13 was released in June 2022 and, at system level, provided permissions for various apps to access photos and videos via the two options ‘Allow all’ and ‘Do not allow’; the ‘Allow limited access’ option was a new feature introduced in Android 14, which was released in autumn 2023;

− The Facebook app’s Manifest file declares the following permissions: READ_MEDIA_IMAGES, READ_MEDIA_VIDEO, READ_MEDIA_VISUAL_USER_SELECTED and ACCESS_MEDIA_LOCATION (relating to EXIF location metadata): if granted via a single system prompt, the authorisation for photos also includes authorisation for location data, without a second request; the Technical Report notes that it is “highly likely” that the app utilises this method, although this cannot be verified;

− the READ_MEDIA permissions, if granted via the “Allow everything” option, enable the app to read all photos and videos, to process them in any way, either locally or in the cloud, and, if the app also has the INTERNET permission (granted to almost all apps upon installation), to transmit them to the provider’s systems; if the user was already using the app at the time of the update to Android 13 and the app had the previous READ_EXTERNAL_STORAGE permission, the READ_MEDIA permissions were automatically granted when the feature was introduced;

− for the publication of a single photo, Android has, since 2023, provided the ‘photo picker’ mechanism, which allows apps to access only the photos selected at that moment without requiring system permissions; the Feature, however, by its very nature requires broader and continuous access, but should have been the subject of a separate request, linked solely to it and disabled by default; Meta, however, has combined multiple features with different access requirements into a single request;

− the Facebook app is proprietary software, the source code for which is not available, and traffic to Meta’s systems is encrypted: the Authority is unable to verify analytically what data is transmitted, nor to rule out

the possibility that the app transmits photos and their associated metadata to Meta's systems without the user's knowledge; a black box analysis of the traffic would be time-consuming, costly and of uncertain outcome.

The Technical Report concluded that the findings fall within the scope of Article 5(3) of the ePrivacy Directive, insofar as access to data takes place via IT mechanisms (e.g. the Android operating system's APIs) and enables Meta to access information stored on the terminal equipment ("gaining access to information already stored in the terminal equipment").

2. INITIATION OF PROCEEDINGS FOR THE ADOPTION OF CORRECTIVE AND PENAL MEASURES AND THE PARTY'S DEFENCE

2.1. Initiation of proceedings (Article 166(5) of the Code)

The notice initiating the proceedings. On the basis of an examination of the evidence gathered during the activities described above and the establishment of the alleged infringements, by a notice dated 29 July 2026 (ref. no. 115205), served in accordance with Article 166(5) of the Code, the Office initiated proceedings for the adoption of the measures referred to in Article 58, paragraph 2, of the Regulations against the data controller, inviting the latter to submit written defences or documents to the Data Protection Authority or to request a hearing before the Authority (Article 166(6) and (7) of the Code, as well as Article 18(1) of Law No 689 of 24 November 1981).

The alleged infringements and the scope of the allegations. The alleged infringements relate to Article 122, paragraphs 1 and 2, of the Code, also in conjunction with Articles 6, 7, 12 and 13 of Regulation (EU) 2016/679, for having accessed information stored on users' mobile devices – specifically photographs, videos and related metadata – without consent or any other valid legal basis, and without having informed the users themselves in a manner that ensures their effective awareness.

The scope of the infringement is limited to all Italian users who have installed the Facebook app on their Android-powered devices.

Access to the case file and extension of the deadline for submitting a defence. By letter dated 5 August 2026 (registered on 6 and 7 August 2026, ref. nos. 119078 and 119465), Meta requested access to the case file and a forty-five-day extension of the deadline for submitting its defence. By letter dated 10 August 2026 (ref. no. 119976), the Office forwarded the sole document not yet in the Company's possession (the internal memo dated 2 December 2025 with three annexes) and granted the extension, setting the deadline for 12 October 2026. By letter dated 14 September 2026 (ref. no. 131503) Meta reported that its security systems had prevented the attachments from being received, as they had been sent in a compressed '.7z' format not accepted by its servers, and that the communication of 10 August had been sent to an incorrect address belonging to one of its legal representatives; it requested that the documents be resent and elected domicile with its Italian solicitors. The Office resubmitted the documentation in PDF format to the correct address on 16 September 2026 (ref. no. 132333).

2.2. Defence Submissions (Article 166(6) of the Code)

Meta's defence submission. By a submission dated 12 October 2026, sent by email and certified email (PEC) and registered on 13 October 2026 (ref. no. 145274), Meta requested that the proceedings be dismissed or that no further action be taken, without requesting a hearing. It produced the special power of attorney (Annex A), screenshots of the Feature's settings (Doc. 1), the notice preceding the authorisation request (Doc. 2), the operating system's authorisation steps (Doc. 3), the updated settings page (Doc. 4) and the financial statements of Meta Platforms Ireland Limited as at 31 December 2024 (Doc. 5).

The defences may be summarised as follows:

− as a preliminary point, the allegations are formulated in general terms, with no connection between the provisions of the Regulation listed in paragraph 6 of the notice of initiation and the observations set out in the body of the notice, thereby seriously prejudicing the right of defence;

− as a main argument, Article 122 of the Code and Article 5(3) of the ePrivacy Directive do not apply, as they would require the use of an electronic communications network and the transmission of information from the device, according to the Company's interpretation of EDPB Guidelines 2/2023 (paragraphs 32, 44 and 53). The Feature would operate entirely on the device (on-device), reading only basic metadata (date and time) and without transmitting any data to Meta's servers, and the processing would be limited to the suggestion made to the user. The Data Protection Authority would thus be basing its argument on a purely theoretical capability of the READ_MEDIA permissions rather than on actual access. Meta also classifies the app as a 'software-based service' rather than an electronic communications network, and presents the publication of the suggested content as a separate 'Publication Phase', initiated by the user and, in its view, outside the scope of the complaint;

− as regards jurisdiction, the allegations relating to Articles 6, 7, 12 and 13 of the Regulation would fall within the exclusive jurisdiction of the DPC, as the lead authority (Article 56 of the Regulation), as there is no exception to the one-stop shop principle (Court of Justice, judgment of 15 June 2021, C-645/19, Facebook Belgium, paragraph 74; EDPB, Opinion 5/2019 of 12 March 2019 on the interaction between the e-Privacy Directive and the General Data Protection Regulation, in particular as regards the competences, tasks and powers of data protection authorities), and Article 122 of the Code, as lex specialis, could not extend the Data Protection Authority's jurisdiction. The Company acknowledges, however, that the e-Privacy Directive does not provide for any one-stop-shop mechanism and that the Data Protection Authority is competent to enforce the national transposition rules, where applicable (submission, §4.1);

− in any event, the operating system authorisation would constitute a positive action on the part of the user and, therefore, free, specific, informed and unambiguous consent, relating to a single purpose (to facilitate the sharing of content) and revocable at any time; a single consent could cover multiple processing operations with the same purpose (Recital 32 of the Regulation; EDPB Guidelines 5/2020). The in-app control ('In-App Feature Toggle') would not constitute a consent mechanism (Memorandum, §4.31) and would not be equivalent to a pre-ticked box (Court of Justice, judgments of 1 October 2019, C-673/17, Planet49, and of 11 November 2020, C-61/19, Orange România). Meta acknowledges, however, that in the past the control might have appeared 'active' before the user granted system authorisation, contrary to what was stated in its reply of 14 November 2025, and reports that it has remedied this with version 581 of the app, specifying that users who have not updated the app continue to see the previous interface (statement of case, §4.33 and footnote 7). It also admits that the authorisation applies "to the App as a whole" and that the Feature "cannot operate on a 'one photo at a time' basis" (statement of defence, §5.35 and §6.2);

− in the further alternative, access would be strictly necessary for a service explicitly requested by the user, namely the "efficient and effective process of uploading photographs" (statement of defence, §4.37), an argument set out in a single paragraph and lacking supporting evidence. As regards the 'photo picker', Meta observes that the suggestion does not correspond to any objection and would in any case be incorrect, because the Feature could not operate 'one photo at a time' and the Android permissions model would not allow requests on a per-feature basis (submission, §6.1–6.3);

− Meta clarifies that it does not base the processing on consent as a legal basis within the meaning of the Regulation, but on contractual necessity (users with full legal capacity) and legitimate interest (users with limited legal capacity, §5.23), bases distinct from the requirements of Article 122 of the Code, and considers the reference to Article 7 of the Regulation to be irrelevant; for access, it would rely solely on express consent via the system authorisation and, in the alternative, on strict necessity. As regards information, users would be informed by the general privacy notice (which, from July 2022, would refer to photo metadata), by the notice preceding the authorisation request, by the sharing suggestion itself, and by the Help Centre article published in April 2026 (§5.32); 'an additional and separate notification' would not be required (§5.31), as the data is 'non-sensitive' and the processing is 'consistent with the main functions of the App' (§5.30). There would be no deceptive design patterns, the name of the Feature would not be misleading, and the ACCESS_MEDIA_LOCATION authorisation, declared in the Manifest at application level, would not be used by the Feature (§5.34–5.36);

− as a very last resort, there would be no harm and the infringement would be of minimal severity, as the data would consist solely of basic, non-sensitive metadata; the estimate of approximately 20 million users cited by the Authority would be unsubstantiated and incorrect, with the Company failing to provide any alternative figure; at most, a non-public notice could be issued.

3. THE AUTHORITY'S ASSESSMENTS

3.1 Regulatory framework and methodological premise

The positions expressed by Meta, both in its response to the request for information and in its defence submission, are not sufficient to rule out Meta's liability in relation to the allegation made and, furthermore, require the Authority to provide the necessary preliminary clarifications regarding the method by which the matter in question has been addressed.

The basis for assessment. The allegation concerns a breach of Article 122 of the Code. It is this provision, and not the Regulation nor the European interpretative framework referred to by Meta, that serves as the basis on which the Authority assesses the conduct: Article 122 defines the prohibited conduct (access to information already stored on the user's terminal without their consent, following prior notification) and is the provision whose breach is punishable under Article 166(2) of the Code. Meta's defences, however, shift the discussion to a different terrain: that of the technical scope of Article 5(3) of the ePrivacy Directive, as interpreted by EDPB Guidelines 2/2023, and that of the provisions of the Regulation. The Authority does not intend to shy away from addressing these aspects, which it examines in detail in the following paragraphs. It considers it necessary, however, to reiterate that the legal basis on which the Authority is proceeding is Article 122 of the Code, interpreted in accordance with the Directive which it transposes, and that the Company's comments and the Guidelines referred to are relevant only insofar as they help to clarify the scope of that provision, not in the sense of replacing its text or restricting its scope of application.

With this in mind, the analysis is structured around the elements of Article 122: access to information stored on the terminal (paragraph 3.3), user consent and information (paragraphs 3.5 and 3.7) and exceptions to consent (paragraph 3.6). The Regulation is referred to solely as a substantive benchmark for defining consent and information, by virtue of the reference made by the sector- specific legislation itself (Article 2(f) of the ePrivacy Directive; Article 94(2) of the Regulation), and is not the subject of any separate challenge (paragraph 3.4). The reasons why the challenge concerns paragraphs 1 and 2 and not paragraph 2-bis are set out in paragraph 3.2 of this decision.

The rationale behind Article 122 and the legal interest protected. The method just outlined requires us to clarify, before any other assessment, which interest the legislator intended to protect through Article 122 of the Code and the European provision it transposes, because it is in the light of this purpose that both the scope of the provision and the validity of the Company's defences must be assessed. Indeed, the provision is not a rule on the processing of personal data in the strict sense, but a rule safeguarding the integrity of the user's private sphere: it makes any access by parties other than the user to the user's terminal equipment and to the information stored therein subject to a free and informed choice by the user.

Such is the perspective of the ePrivacy Directive, Recital 24 of which states that the terminal equipment of users of electronic communications networks and any information stored on such equipment form part of users' private sphere, which requires protection under the European Convention on Human Rights, and that so-called spyware, 'web bugs', hidden identifiers and other similar devices may be introduced into the user's terminal without their knowledge in order to gain access to information, store hidden information or track the user's activities, and may constitute a serious intrusion into that user's private life; the use of such devices, the recital adds, "should be permitted solely for legitimate purposes and the user concerned should be aware of it". In this regard, the Court of Justice has clarified that Article 5(3) "refers to the 'storage of information' and to 'access to information already stored', without qualifying that information or specifying that it must be personal data", and that the provision "therefore aims to protect the user from any interference with their private life, regardless of whether or not that interference concerns personal data" (Planet49, paragraphs 68–69). Referring to recital 24, the Court added that such protection "applies to any information stored on such a terminal device" and is intended to protect users from the risk that hidden identifiers or other similar devices might be introduced into the terminal "without their knowledge" (paragraph 70).

Protection under national law and the protected interests. The national legislature has adopted the same approach: the explanatory report accompanying the draft of Legislative Decree No 69 of 28 May 2012 (hereinafter 'the explanatory report') explains that the reform of Article 122 aims to ensure that users are 'better informed' about what happens to their data and can 'exercise greater control over it'. There are therefore two closely linked protected interests: the confidentiality of the device and the information it

contains, and the user's self-determination, that is, the effective ability to know who is accessing their device, what information is being accessed, and for what purposes, and to choose whether to allow such access. The EDPB's Guidelines 2/2023 summarise this dual protection by stating that the Directive protects users' privacy "not only in relation to the confidentiality of their information, but also by safeguarding the integrity of the terminal equipment" (para. 14; see also
para. 8). It follows from this objective that protection is provided in advance and is independent of proof of harm, the transmission of information and the more or less sensitive nature of that information (see para. 3.3). The genuine risk identified during the preliminary investigation. In light of this purpose, the preliminary investigation highlighted a genuine risk to the protected interests. The Technical Report noted that the READ_MEDIA permissions requested by the app, granted via a single system pop-up window in the form of 'Allow all', enable Meta to read the device's entire photo and video library, to process it locally or in the cloud and, since the app also has the INTERNET authorisation, to transmit it to its own systems; that the access granted is, as a rule, permanent and revocable only via the device's settings; that the authorisation regarding photos may include, without a second request, access to location metadata (ACCESS_MEDIA_LOCATION); and that the app is closed-source software with encrypted traffic, meaning that neither the user nor the Authority is able to verify what information is actually being read and transmitted, and verification is, from a technical perspective, dependent on the full cooperation of the data controller. It should in fact be noted that a smartphone's media library is one of the most private aspects of a person's digital life: it contains images and videos of private and family life, often including third parties and minors, which the user never intended to make accessible to a service provider. It should be clarified, however, that the Authority has not established that the Feature accesses location data, that the content is transmitted or used for further purposes, nor that special categories of data are processed, and these assumptions do not form the basis of the decision. However, the investigation has shown – and the Company has not refuted this with any technical evidence – that the conditions for such outcomes were created by Meta: broad, continuous and unverifiable access, obtained through an authorisation requested for other purposes and lacking specific consent for the Feature. This is the threat to the user's privacy that Article 122 aims to prevent.

Broad and continuous access. Hereinafter, 'broad' access refers to that made technically possible by the READ_MEDIA authorisations granted in the 'Allow all' format, which enable the app to read all photographs and videos on the device and not just those selected by the user (Technical Report, para. 1.1); 'continuous' means that the authorisation, once granted, generally remains valid until the user explicitly revokes it in the system settings (ibid., para. 1.1 and note 3), and not that the Feature continuously reads the archive. The scope is therefore a characteristic of the authorisation and of the technical capability it confers on Meta, not of the use that the Feature makes of it, which, according to Meta, is limited to the most recent content and basic metadata (memorandum, §4.17) and which the Authority is unable to verify.

Limited access. Selecting the 'Allow limited access' option, introduced with Android 14 (READ_MEDIA_VISUAL_USER_SELECTED permission), restricts access to only the content selected by the user. For the Authority, this restriction makes no difference: Article 122 applies to any access to information stored on the device, without limits on duration or quantity (EDPB Guidelines 2/2023, para. 37); the choice relates to the app as a whole and not to individual features, and therefore does not confer specificity on the consent; the option is not available to users of Android 13 and earlier versions; and access to the subset remains permanent unless revoked, whilst any change to it requires the procedure to be repeated, which effectively leads to the granting of the broadest possible authorisation (Technical Report, para. 1.4). The limited nature of access therefore affects, at most, the extent of the interference (see para. 6.2), not the existence of the infringement, nor the lack of specificity or inadequate information (paras. 3.5 and 3.7).

The content of Article 122 of the Code. Article 122(1) of the Code, which transposes Article 5(3) of the ePrivacy Directive, permits the storage of information on a subscriber's or user's terminal
equipment, or access to information already stored, only on condition that the user has given their consent after being informed in a simplified manner. Consent may also be given through specific settings in software or devices, provided that these are easy and clear for the user to use (Article 122(2)). Article 122(2-bis) prohibits, subject to the provisions of paragraph 1, the use of an electronic communications network to access information stored on the terminal equipment. The only exceptions to the requirement for consent are storage or technical access solely for the purpose of transmitting a communication over an electronic communications network, and those strictly necessary for the provider of an information society service

explicitly requested by the user. The text of paragraph 1, which, according to the explanatory report, faithfully reproduces that of Article 5(3) of the Directive as amended by Directive 2009/136/EC, prohibits access to information already stored in the terminal without requiring, for the purposes of such access, that the information leave the device, nor that an electronic communications network be used. It should also be noted that the reference to the network is specific to paragraph 2-bis alone, which, as is evident from the preparatory work (minutes of the 14th Committee of the Chamber of Deputies, sitting of 17 May 2012, Government Act No. 462), retains the general prohibition already provided for in paragraph 1 in its previous wording and is not the subject of the challenge, which concerns paragraphs 1 and 2.

The concept of consent. The concept of consent required by Article 122 is not an independent one: Article 2(f) of the ePrivacy Directive identifies it with the data subject's consent as defined by the Regulation, that is, a freely given, specific, informed and unambiguous indication of the data subject's wishes, expressed by a statement or a clear affirmative action (Article 4(11) of the Regulation), accompanied by the conditions set out in Article 7 and recitals 32 and 43 (see EDPB, 'Guideline 5/2020 on consent under Regulation (EU) 2016/679', version 1.1 of 4 May 2020; Planet49 and Orange România). Consent must be given for each distinct purpose and cannot result from silence, inactivity or pre-ticked boxes.

The proactive and active nature of consent and information. Article 5(3) of the Directive and Article 122(1) of the Code require that the user be informed and give consent prior to access, and that consent result from active behaviour and cannot be presumed: first information, then consent, then access. Developments in case law and their application to the present case are set out in paragraphs 3.5 and 3.7 of this decision.

Guidelines 2/2023 and their interpretative authority. The technical scope of Article 5(3) of the Directive is clarified by EDPB Guidelines 2/2023, according to which the provision applies whenever an entity takes measures to gain access to information stored on the terminal, regardless of the origin of the information, and, typically, when it sends instructions to the terminal to receive the information in return (paragraphs 30–33); the local use of information by an application via system APIs does not constitute access as long as the information does not leave the device; however, when such information or any derivative thereof is accessed, Article 5(3) of the aforementioned Directive would apply (paragraph 44); local processing and client-side code are relevant where the information processed is made available to third parties, for example, sent to a server on the instructions of the entity providing the code (paras. 52–53); the applicability of the provision does not automatically imply an obligation to obtain consent; it is necessary to verify whether an exception applies (para. 56). Article 122 of the Code is not, however, limited to so-called tracking tools: the provision governs access to information already stored, regardless of the technology used (see Guidelines on cookies and other tracking tools of 10 June 2021, at www.gpdp.it web doc. no. 9677876). Guidelines 2/2023 constitute a soft-law instrument of the EDPB: they are an authoritative interpretative aid, which the Authority considers and discusses in detail (see below), but they do not bind the application of Article 122, the scope of which is determined on the basis of the wording of the provision and the Directive it transposes, their purpose and the case law of the Court of Justice, and cannot be restricted by way of interpretation on the basis of guidance not contained in the text.

Evidence, information and sanctions. From an evidential perspective, the data controller must be able to demonstrate the lawfulness of processing operations and that valid consent has been obtained (Articles 5(2) and 24 of the Regulation). With regard to information, Articles 12 and 13 of the Regulation set out the criteria of conciseness, transparency, intelligibility and accessibility against which the information provided 'in a simplified manner' under Article 122(1) of the Code is assessed. As regards sanctions, a breach of Article 122 of the Code is punishable under Article 83(5) of the Regulation (Article 166(2) of the Code). This framework is consistent with Article 15a of the Directive, which requires Member States to establish effective, proportionate and dissuasive sanctions for breaches of national implementing rules (paragraph 1), to confer on the competent authority the power to order the cessation of infringements (paragraph 2) and to endow it with the necessary powers, including the power to obtain any relevant information (paragraph 3).

3.2 Timeliness, the right to be heard, the general nature of the allegations and identification of the data controller

Observations on the right to be heard. The Authority examined the preliminary investigation documents (the complaint, the request for information and Meta's response, the Technical Report, and the notice of initiation) and the defence submission, which it considered in full, including with regard to the points on

which Meta reserved the right not to recognise the Authority's jurisdiction. The right to be heard was fully guaranteed: Meta had access to the entire file, was granted an extension of forty-five days beyond the standard thirty-day deadline (Article 166(6) of the Code) and, when it stated that it had been unable to open the attachments sent in compressed format due to a specific feature of its systems, the documentation was resent well in advance of the deadline.

The alleged vagueness of the allegation. The notice of initiation alleges a breach of Article 122 of the Code and, after describing the facts in detail (paragraphs 2 and 3), sets out the grounds for the unlawfulness in distinct categories: the absence of specific consent for the Feature, distinct from that relating to the app's other features; the inadequacy of the legal bases invoked by Meta; the lack of information provided to existing users and of specific information in the privacy notice and within the product; the procedures for requesting authorisation (paragraph 4). The reference to Articles 6, 7, 12 and 13 of the Regulation, introduced by the phrase 'also in relation to', refers to the substantive criteria by which, pursuant to Article 2(f) of the ePrivacy Directive and Article 122(1) of the Code, user consent and information are assessed. The complaint therefore enabled the Company to identify the facts and the provisions allegedly breached, as demonstrated by the thoroughness with which Meta responded to each point (paragraph 2.2). The preliminary objection must therefore be dismissed, it being understood that, for the reasons set out in paragraph 3.4, no independent breaches of the provisions of the Regulation have been established.

The scope of the allegation. The notice of proceedings alleges a breach of Article 122, paragraphs 1 and 2, of the Code, but not of paragraph 2-bis. Paragraphs 1 and 2 set out the rule of conduct relevant here: the storage of information on the terminal and access to information already stored are permitted only on condition that the user has given their consent after being informed, in accordance with the procedures laid down in that provision. The Authority has therefore based the charge on what has been technically proven and is not disputed by the data controller: the app's ability to access, by virtue of the authorisation granted, the multimedia content on the device, in the absence of specific consent and adequate information. This delimitation complies with the principle of
correspondence between the charge and the decision, which requires the Authority to rule solely on the facts and the provisions alleged against the Company in the notice of proceedings, in order to safeguard its right of defence (Article 166(5) and (6) of the Code). This decision does not preclude paragraph 2- bis from contributing to the definition of the scope of protection, nor does it mitigate the seriousness of the conduct, which remains the same and is entirely attributable to Article 122, paragraphs 1 and 2; it merely avoids shifting the focus to an element – the use of the network – which is not necessary to establish the infringement and to which the Company has attempted to attribute the entire dispute, despite having failed to provide conclusive technical evidence.

Identification of the data controller. As regards the identification of the data controller, the notice of proceedings contains, due to a typographical error, the name Meta Platforms Technologies Ireland Limited. However, Meta Platforms Ireland Limited has declared itself to be the data controller responsible for the Feature and the party to whom the request for information and subsequent communications were addressed; it received the notice of initiation, exercised its right of access and fully presented its defence, without alleging any prejudice. The error therefore did not affect the right of defence. It follows that this decision is adopted in respect of Meta Platforms Ireland Limited.

3.3 Applicability of Article 122 of the Code, the Data Protection Authority's jurisdiction under the ePrivacy Directive and the non-application of the cooperation and consistency mechanism provided for in the Regulation

Although it is evident from the entire investigation that the approach adopted by Meta implies a framing of the Feature exclusively from the perspective of the obligations under the Regulation (for example, see the legal bases referred to in the privacy notice), the Authority, in light of the analysis carried out, considers that the special provisions set out in the ePrivacy Directive and the corresponding domestic transposing legislation must be fully applied.

That said, the scope of the investigation is limited to the stage of accessing information stored on the terminal and the related consent and information (Article 122 of the Code). Articles 6, 7, 12 and 13 of the Regulation are referred to solely as substantive criteria (Article 2(f) of the Directive) and do not form the subject of a separate challenge, nor do the general principles and obligations of the Regulation referred to below for

interpretative and evidential purposes only (see paragraph 3.4).
Meta's arguments. In its defence submission, Meta argued that "the Data Protection Authority has no jurisdiction to supervise or carry out enforcement activities against Meta in relation to the functionality, since Article 122 of the Code (and, by extension, Article 5(3) of the ePrivacy Directive) does not apply".

In support of its position, Meta refers, from a legal perspective, to paragraphs 23, 32 and 44 of the "Guidelines 2/2023 on the technical scope of Article 5(3) of the ePrivacy Directive" (Version 2.0, adopted on 7 October 2024 by the EDPB), emphasising the passage which states that information must leave the device for there to be access to information already stored.

Furthermore, the Company contends that there is also no transmission via an electronic communications network, as in the present case we are dealing with an application that interacts locally with stored data, constituting "a software-based service, and not an electronic communications network within the meaning of Article 5(3) of the ePrivacy Directive".

From a functional perspective, Meta asserts that the irrelevance of Article 122 of the Code to the present case is demonstrated by the fact that the Feature:

- operating exclusively on-device, reads the photo gallery and the related metadata (limited to date and time) stored therein, in order to suggest to the user the most recent multimedia content to post on Facebook;

- during this process, Meta's servers do not collect or store any data relating to the gallery;

- the processing relating to the Feature concludes with the suggestion to the user to post; and

- the posting constitutes a separate and subsequent stage (the so-called 'Posting Stage'), initiated by the user.

Meta's objections, which are based on the alleged absence of a network, the need for the information to leave the device and the exclusively local nature of the Feature, are examined in the following order:
the scope of application of Article 122 of the Code;
the existence of access in the present case;
the statements by which Meta itself refutes the premise of solely local processing;
evidence of the absence of transmission;
and, finally, the Authority's jurisdiction and the non-application of the cooperation and consistency mechanism.

The scope of application of Article 122 of the Code. From a systematic perspective, the smartphone on which users' photos and videos are stored constitutes, to all intents and purposes, a network terminal equipment within the meaning of European and national legislation. Furthermore, the fact that the information is generated and initially stored locally does not, in this respect, preclude the applicability of Article 122 of the Code on the protection of personal data, nor of Article 5(3) of the ePrivacy Directive, since access to such information takes place via IT mechanisms, the Android operating system APIs declared in the Manifest file, which technically enable Meta to access the information on the device and subsequently transmit it over the network. The Manifest file declares the application's technical capability to access this information (READ_MEDIA_IMAGES and READ_MEDIA_VIDEO permissions); its actual activation depends on the user granting authorisation, a fact which Meta itself acknowledges (see below, paragraph 3.5). EDPB Guidelines 2/2023 expressly include the smartphone amongst terminal equipment (paragraph 17).

The concept of an electronic communications network. It is irrelevant that Meta classifies the app as a 'software-based service' rather than an electronic communications network. Article 5(3), in its current version, does not make the application of the provision conditional upon the use of a network to access information: the EDPB has observed that the 2009 amendment specifically removed the reference to the 'use of an electronic communications network', thereby extending the protection to terminal equipment (Guidelines 2/2023, para. 15). Similarly, Article 122(1) of the Code, which transposes the provision, contains no reference to the network; such a reference appears only in paragraph 2-bis, which is not the subject of the dispute. Access is also facilitated by software that Meta distributes to the terminal and which operates in accordance with the instructions it has drawn up, a scenario which the EDPB includes amongst those constituting access (paras. 32 and 33); and the Technical Report describes the app as a client 'continuously

connected to Meta's cloud'. Moreover, the concept of an electronic communications network referred to by Meta is neutral with regard to transmission technologies and broad enough to cover any type of infrastructure (Guidelines 2/2023, paragraphs 23–24), so that the Company's argument is not supported even from a definitional perspective.

The EDPB's Guidelines 2/2023 must be read in their entirety, and not merely in the passage cited by the Company. They specify, first and foremost, that the applicability of Article 5(3) is not limited to the scenario transmission, but applies whenever the entity takes measures to gain access to stored information (para. 32), as is the case with the acquisition, upon first use of the app, of a broad and permanent authorisation, in the form of 'Allow everything' that the system prompt leads the user to select, to the entire multimedia archive (Technical Report, paras. 1.1 and 1.4); that the concept of information does not depend on the source or the manner in which the information has been stored (paras. 12, 31 and 39); that there are no limits on duration or quantity (para. 37); that protection does not depend on the user's awareness (para. 20) and that consent is required even when accessing a read-only value via the operating system API (para. 11, which refers to Opinion 9/2014 of the Article 29 Working Party ("WP29") on device fingerprinting). As regards paragraph 44, it states that the use of information by a local application via system APIs would not constitute 'access' 'as long as the information does not leave the device', but adds that 'when such information or any derivative thereof is accessed, Article 5(3) would apply'. This passage cannot therefore be interpreted as a general exemption for applications that read local files: it concerns the scenario of use strictly confined to the device itself and linked to a strict necessity, a factual condition which the Company has not demonstrated (see below); this is without prejudice to access to information "or any derivative thereof", such as suggestions generated by the app's selection of content and related metadata, which, if the user were to publish them on the platform, would in any case become known to Meta; and, in any event, the document states that it does not examine the derogations (paragraphs 4, 40 and 56).

The characteristics outlined above fall squarely within the scope of Article 122 of the Code, as set out in paragraph 3.1, which makes access to information already stored on the device subject to the user's informed consent, without requiring that the information leave the device or that an electronic communications network be used.

Access in the present case. The Feature allows Meta to 'access the image gallery on users' devices', enabling the app to analyse their multimedia content and to present 'basic sharing suggestions from the user's gallery whilst they are browsing Facebook'. The photographs, videos and related metadata stored in the smartphone's memory are information already stored on the user's terminal device, regardless of their origin. Furthermore, once the user has granted the READ_MEDIA permissions without restrictions ('Allow everything'), the Facebook app can read the entire shared multimedia archive (Technical Report, para. 1.1). Moreover, Meta itself describes how the Feature operates as a reading of such information: once the Feature has verified the presence of the system authorisation and the activation of the in-app setting, it "queries the device's gallery index to identify the most recently added items and selects one of them in order to generate a sharing suggestion" (statement, §4.17). This constitutes access to information stored on the device, within the meaning of Article 122. Such access is carried out via Meta's software, which reads and selects the content, prior to and irrespective of any choice made by the user. In this context, the natural and expressly stated purpose of this Feature is the publication of the suggested content on the user's profile: otherwise, the very usefulness of the Feature would in fact be null and void. It follows that the processing carried out by Meta consists of two sequential stages—access to stored data and publication—which are inextricably linked, of which only the first is the subject of examination here.

The Android permissions model. Meta's argument, according to which the Company does not have access to data in the course of the Feature's operation, is refuted by the Android system's permissions model, which is the subject of this investigation. As stated by the Company itself in
its defence, "the Android permissions model does not allow apps to request access to media content on an individual basis for each feature. The Operating System-Level Permission applies to the app as a whole, and the scope relevant for such access is always under the user's full control (e.g., full access or access limited to selected items only)". As for the option to choose limited access, which does not alter this conclusion, see below, paragraph 3.5. It cannot therefore be argued that Meta has access to the multimedia content of users who have authorised the Facebook app at operating system level, whilst such access would not apply to the Feature, which is integrated into the same app: the authorisation to access the gallery applies to the entire app. It follows that the general authorisation granted to post a photo enables the app, and therefore Meta, to

read the gallery for the Feature as well. In any event, in the Authority's view, the limited nature of the access makes no difference for the purposes of the infringement.

The 'Publishing Phase'. Conversely, it is irrelevant that the publication of the suggested content takes place on the user's initiative (the so-called 'Publishing Phase', as defined by Meta). The Authority does not contest this phase in itself, but rather the access that precedes it, for three reasons. Firstly, the scanning of the archive, the selection of the content and its presentation to the user are carried out by Meta before the user has made any choice. The subsequent decision to publish occurs after access has already taken place and cannot constitute the consent required by Article 122, which must be prior, specific and informed with regard to the access itself. Furthermore, the Feature, which is preset as active, applies to all users who have granted system authorisation, including those who will never publish the suggested content: for these users, access is based solely on system authorisation, granted for a different purpose, without any voluntary act specifically relating to the Feature. Finally, Meta argues that the authorisation has a 'single purpose', namely to facilitate sharing, in order to assert its validity as consent (memorandum, §4.27–4.28), whilst at the same time maintaining that access and publication are distinct processing operations, in order to exclude the applicability of Article 122 (§4.14–4.16). The two positions are irreconcilable: if the purpose is singular, access is the first act of a single operation; if the stages are distinct, the general authorisation does not cover the Feature and is not specific.

Meta's statements and the premise of processing being solely local. Meta's defences rest on a premise: according to the Company, the first part of the Feature – ranging from access to the gallery to the selection and proposal of the suggestion – does not constitute processing attributable to Meta (memorandum, §4.14–4.17). This premise is contradicted by the very information that Meta provided to the Office and to users.

The letter of 14 November 2025. Given these premises, the information the Company provided in its letter of 14 November 2025 (ref. no. 152086/25) is, first and foremost, surprising, as it raises doubts about the consistency of the various versions provided. In response to an explicit enquiry from the Office regarding the legal bases for the processing carried out via the Feature, Meta stated: "For the processing of personal data for the purpose of providing the Feature, Meta relies on the necessity to perform a contract for users who have the legal capacity to enter into a binding contract, and on legitimate interest for underage users who have limited capacity to enter into a binding contract". Leaving aside the substance of the response, which will be analysed later, if Meta did not process users' data via the Feature, there would be no reason to identify and disclose the relevant legal bases: this obligation arises only if processing actually takes place, and processing takes place when the information retrieved from a local storage device enters the sphere of control of the data controller (who is distinct from the person who physically holds the storage device) who uses it for the specified purposes. Meta has also attributed these legal bases to the processing carried out 'to provide the Feature', and not solely to the subsequent stage of publication.

The terms Meta uses to describe the Feature. The same note also contains phrases describing the first part of the Feature as an activity carried out by Meta: "Meta presents the user, whilst browsing Facebook, with basic sharing suggestions drawn from their gallery"; "When a user grants Meta access to their gallery via their device settings […] Meta gains local access to the gallery on the user's device […] Meta processes multimedia content from the user's gallery in connection with the Feature […] Meta also processes basic metadata relating to the aforementioned multimedia content in the gallery, such as the date and time the photo was taken, photos marked as favourites by the user, and the type/orientation of the photo (for example, panorama, time-lapse). Meta processes this information to show the user basic sharing suggestions"; and further: "Should a user disable the 'Share suggestions from gallery' setting (see Figure 1) without changing the general settings of the device's gallery, Meta ceases to process information from the user's gallery in relation to the Feature". The adjective "local" describes the method of access and does not exclude Meta's liability: the Company identifies itself, and not the user or the operating system, as the entity that 'gains access' to and 'processes' the content, and does so, by its own description, 'to show the user sharing suggestions', that is, for a purpose that precedes and is independent of publication. The information provided by Meta to describe how the Feature works therefore reveals processing activities which the Company itself states it carries out and which fall within the scope of Article 122 of the Code, in stark contradiction to the defences set out in its written submissions.

The information provided to users. The information provided to users supports this view. As stated by the Company in its written submissions, the Privacy Policy, in the section 'What information do we collect?', includes a menu entitled 'Information about apps, browsers and devices', which explains the information

present on devices that Meta collects and receives ('We collect and receive information from the devices you use and relating to them, as well as to your use of them. Here is some of the information we collect and receive about devices: […] Information you share with us via your device settings, such as GPS location, camera access, photos and related metadata […]"). By clicking on the 'related metadata' link, the user reads that "[…] if you grant us permission to access the photos on your device, we collect metadata. This metadata comes from and contains information about your photos and videos, including the date and time you created them. We use it to do things such as remind you when you have new photos to upload'. According to Meta, this wording, 'which has been included in the Privacy Policy since July 2022, expressly covers the features of the Functionality'. If this is the case, it follows that Meta 'collects' the metadata from the photos, and the privacy notice itself is incompatible with the argument that processing takes place exclusively locally. It is one or the other: either the metadata is collected by Meta, in which case Article 122 applies; or it is not, in which case the privacy notice – which Meta considers sufficient to inform users – inaccurately describes the processing. Even in the 'Sharing suggestions from your gallery' settings, Meta informs users that 'when you authorise Facebook to access your device's gallery to post photos and videos, we use basic metadata (e.g. when the photos were taken or which ones have been added to favourites) to provide sharing suggestions from your gallery whilst you're browsing Facebook'. Here too, it is Meta that 'uses' the metadata, and does so to provide suggestions to the user, not to post them.

The processing attributable to Meta. Consequently, the processing carried out by Meta through the Feature, and the fact that the Company accesses information stored on users' devices – even if only in relation to metadata – are indisputable on the basis of the Company's own statements and documents. It remains the case, in any event, that Article 122 does not make its application contingent upon the operation being classified as the processing of personal data by the data controller: the provision protects the user from 'any interference with their private life', regardless of whether or not it concerns personal data (Planet49, paragraphs 68–69). The foregoing considerations therefore serve to refute Meta's premise and to further confirm the right of access, not because the existence of the infringement depends on them.

Access irrespective of transmission and harm. It should first be clarified that, even if one were to accept that the information does not leave the device, the protection afforded to users by the legal system is anticipatory: the provision does not require that access result in the harmful use of the information, nor that it be disclosed; interference with privacy occurs as soon as a third party gains the ability to read the contents of the device without the user having chosen or understood this. Proof of actual harm, as invoked by Meta, is therefore not required for the infringement to be established, nor is the transmission of information a condition for the interference to occur, because what the legislator seeks to prevent is the user losing control over who accesses their device and for what purposes. Secondly, Article 122 does not distinguish on the basis of whether the information is more or less sensitive: the severity of the interference may be relevant for the purposes of the penalty, but not for the existence of the infringement. Consequently, the Company's narrow interpretation— which reduces the issue solely to 'basic metadata'—cannot be accepted: what is at stake is not the nature of the metadata accessed, but the extent of Meta's power to access users' devices. For the same reason, the existence of the infringement does not depend on the scope of the authorisation granted: Article 122 also applies to access to a subset of content, such as that permitted by the 'Allow limited access' option; the scope is relevant for the purposes of the information required (paragraph 3.7) and the seriousness of the infringement (paragraph 6.2).
Moreover, the fact that the information does not leave the device – on which Meta bases its defence – has not in any event been proven, as explained below.

The opacity of the app and the failure to provide technical evidence. It should in fact be emphasised that the Technical Report found that the app is closed-source software, the code for which is not available, and that traffic to Meta's systems is encrypted, meaning that the Authority cannot ascertain what data is transmitted. Meta, despite having been urged in the notice initiating the proceedings to provide all documentation necessary to exclude or limit its liability, merely stated that 'no data' is transmitted, without producing any technical evidence (description of the architecture, traffic logs, independent certifications or audits): documents 1 to 4 attached to the defence brief are merely screenshots of the interfaces. In the face of this lack of evidence, the Authority has evidence of the technical authorisations declared in the Facebook app's Manifest.
The principle of accountability. The failure to produce technical evidence is not insignificant, as it lies at the heart of the principle of accountability. The opacity of a proprietary and encrypted system creates an information asymmetry between those who design and manage it and those who are affected by it: it is the

very same asymmetry that separates the controller from the data subject, who is unable to verify which items of information from the photo library are actually accessed and transmitted, and that separates the controller from the supervisory authority, which, like the user, is faced with a closed system of which it knows only what the controller decides to disclose or what it can infer from external sources. From this perspective, the Regulation does not ignore this
asymmetry, but draws the opposite conclusion to that envisaged by Meta: since only the data controller knows and controls the architecture of the processing and has the means to document it, it is incumbent upon them to demonstrate compliance (Articles 5(2) and 24 of the Regulation) and to cooperate with the Authority by providing the requested information (Article 31 of the Regulation; Article 157 of the Code). For systems of this kind, the Authority requires the fullest possible cooperation from the data controller, who is obliged to provide technical evidence to substantiate their claims. The data controller cannot, therefore, exploit to its own advantage the lack of transparency resulting from its own technical choices: if this were the case, the confidentiality of the code and the encryption would become a shield capable of shielding the processing from any scrutiny, and the information advantage that Meta holds over users would extend, with far greater effect, to the Authority tasked with protecting them. The same asymmetry arises, on a much larger scale, for the group of users concerned, which, according to the estimate referred to in paragraph 3.8, runs into the millions.

This is not a matter of reversing the burden of proving access, which the Authority has established on the basis of the authorisations declared by the app, the Technical Report and Meta's own statements. It is a matter of placing on Meta the burden of proving the fact it invokes to its own exclusion, namely that the information does not leave the device – a circumstance that falls entirely within its sphere of knowledge and control. It should be emphasised, in this regard, that, given the substantial body of evidence referred to above (the passages from the privacy notice and the response to the request for information demonstrating processing by Meta and the permissions used by the app, the scope of which see below), it was incumbent upon Meta to describe 'in detail', as expressly requested by the Authority, the technical functioning of the Feature. Instead, the Company's response was surprisingly limited to an apodictic statement—unproven and unverifiable, and at odds with its previous statements (subject to the provisions of Article 168 of the Code)—regarding which the Authority would be expected to take it on faith.

The passage from the Technical Report cited by Meta. Nor is the passage from the Technical Report, referred to by Meta, valid, according to which the Feature would be "theoretically feasible" without the data leaving the device: mere theoretical possibility does not prove that it is actually implemented in this way, and the passage itself notes that, 'in practice', the authorisations used by the app enable Meta to access all photos and their metadata and to transmit them without the user being aware of it.

In light of the foregoing, the Authority considers that access to information stored on the device, within the meaning of Article 122 of the Code, occurs in the present case. The Feature forms part of a single, integrated process (obtaining broad authorisation to access the multimedia library, selecting content, suggesting and transmitting the chosen content to Meta) which Meta itself describes as serving a single purpose, and in respect of which it has neither proven, nor offered to prove, that the information in the library is not made available to Meta prior to publication. This applies regardless of whether the subsequent publication is voluntary, as this does not affect the access phase or the need for prior consent.

The Data Protection Authority's jurisdiction and the non-application of the one-stop shop. With regard to jurisdiction, Meta itself acknowledges that the ePrivacy Directive does not provide for a one-stop shop mechanism and that the Data Protection Authority is competent to enforce the transposition provisions where applicable (submission, §4.1): the question of jurisdiction is therefore entirely resolved by the question of the applicability of Article 122.

Opinion 5/2019 and the Facebook Belgium judgment. The very documentation cited by Meta
confirms this conclusion. In Opinion 5/2019, the EDPB clarified that the authority designated by national law as competent under the ePrivacy Directive has the competence for the
directly apply the national transposition provisions (paras. 77 and 90); that Article 5(3) contains a special provision concerning the storage of and access to information on the terminal (para. 75); that the cooperation and consistency mechanisms of the Regulation "do not apply to the implementation of the provisions contained in the ePrivacy Directive as such" (paragraphs 80 and 91); and that processing operations prior to and subsequent to those not governed by a special provision of the Directive remain subject to the

Regulation, and therefore to the one-stop shop (paragraphs 75 and 84). Similarly, in the Facebook Belgium judgment, cited by Meta, the Court, referring specifically to Opinion 5/2019, stated that "the storage and reading of personal data by means of cookies fell within the scope of Directive 2002/58/EC […] and not within the 'one-stop shop' mechanism', whilst the preceding operations and subsequent processing activities fall within the scope of the Regulation (Facebook Belgium, paragraph 74). This distinction is consistent with the scope of the investigation, which the Authority has limited to the access phase (see above) without affecting the competence of the Irish authority regarding subsequent processing, which it does not examine.

The Authority's powers and the 'ne bis in idem' principle. As regards powers, the EDPB noted that the authority designated to implement the ePrivacy Directive cannot automatically avail itself of the powers under the Regulation, but must derive its tasks and powers from national law (para. 66): under Italian law, these are set out in Articles 157 and 166 of the Code, which refer to the related powers laid down in Article 58(1) and (2) of the Regulation. As regards the need for consistency between the competent authorities for the two instruments, aimed at avoiding breaches of the 'ne bis in idem' principle (paragraph 78), this is satisfied in the present case, as the sole subject of the complaint is the breach of Article 122 in relation to Italian users who have installed the Facebook app on a device running the Android operating system.

The Italian Authority is therefore competent, pursuant to the Code, to establish the infringement of Article 122 in respect of Italian Facebook users on Android devices, the scope to which the notice of initiation has limited the allegations.

3.4 Application of the Regulation in the present case

Meta disputes the alleged infringements put forward by this Authority regarding the legal basis for processing and the privacy notice, arguing that "the Data Protection Authority has neither jurisdiction nor competence regarding the application of, and/or monitoring compliance with, the GDPR by Meta in relation to the functionality".

The Company further stated that any processing carried out in relation to the Feature falls within the scope of the Regulation and, therefore, falls under the jurisdiction of the Irish Data Protection Authority.

The misunderstanding into which Meta has fallen stems from the fact that, according to the Company's account, the Data Protection Commissioner purports to verify the compliance of the processing operations under scrutiny with the provisions set out in Articles 6, 7, 12 and 13 of the Regulation.

This objection misses the mark and is, quite clearly, the result of a misunderstanding.
In reality, the Data Protection Commissioner intended to challenge solely the breaches of Article 122 of the Code, including with regard to the legal basis and the information notice required by that very provision.

The content of the notice of initiation. In its notice of initiation of proceedings pursuant to Article 166 of the Code, the Data Protection Authority did, in fact, raise the issue of a possible breach of
'Article 122(1) and (2) of the Code, also in relation to Articles 6, 7, 12 and 13 of Regulation (EU) 2016/679, for having accessed information stored on users' mobile devices, specifically, videos and related metadata, without the required consent or any other valid legal basis, and without having informed the users themselves in a manner that ensures their effective awareness'.

Moreover, it is the very wording of Article 122 of the Code that refers to 'consent' as the legal basis for the relevant processing, consent which the user may give 'after having been informed in a simplified manner'.

From a systematic perspective, it is worth noting the wording of the ePrivacy Directive, which, in Article 2(2)(f), does not directly define 'consent' but expressly refers to the provisions of the then 'Directive 95/46/EC' (now the Regulation).

Furthermore, the wording of Article 5(3) states that "the storage of information or access to information already stored in a subscriber's or user's terminal equipment shall be permitted only on condition that the subscriber or user concerned has given his or her prior consent, having been informed in a clear and comprehensive manner, in accordance with Directive 95/46/EC, inter alia, of the purposes of the processing".

Therefore, it is the same relevant legislation which, in order to provide substance to the concepts referred to in Article 122 of the Code, through Article 5(3) of the ePrivacy Directive, refers to the provisions of the Regulation in relation, in the present case, to the legal basis of the data subject's consent and the privacy notice.

Consequently, far from claiming jurisdiction over the application of the Regulation in cross-border processing operations for which other authorities are competent, the Data Protection Authority has challenged Meta solely on the grounds of a possible breach of Article 122 of the Code in relation to Italian users. The references to the articles of the Regulation, like those made in the ePrivacy Directive, are therefore merely explanatory of the specific aspects of Article 122 of the Code that are deemed to have been breached, as is also clear from the wording of the relevant passages in the notice initiating proceedings pursuant to Article 166 of the Code.

The case law of the Court of Justice on consent. This approach is consistent with the case law of the Court of Justice, according to which the consent referred to in Article 2(f) and Article 5(3) of the ePrivacy Directive must be read in conjunction with the concept of consent under Directive 95/46 and, today, with Article 4(11), and Article 6(1)(a) of the Regulation (Planet49, paragraphs 50, 57 and 60–63). The reference to these concepts serves to give substance to the requirement of consent laid down in Article 122 and does not transform the challenge into a challenge to the Regulation. In the same vein, Article 1(2) of the ePrivacy Directive provides that its provisions 'clarify and supplement' Directive 95/46, references to which are now deemed to refer to the Regulation (Article 94(2)), and the EDPB has clarified that the consent requirements of the Regulation do not constitute an 'additional obligation' within the meaning of Article 95, but rather preconditions for lawfulness, applicable to situations falling within the scope of the ePrivacy Directive (Guidelines 5/2020, para. 7; see also Opinion 5/2019, para. 40).

The competence of this Authority and that of the lead authority. Nor does the reference to concepts in the Regulation deprive this Authority of its power of assessment. The Court of Justice has held, in a different but significant context, that no provision of the Regulation prevents an authority acting on the basis of its own competence from finding, in the exercise of its functions, that processing does not comply with that Regulation, and that, in so doing, it does not take the place of the supervisory authorities nor does it exercise the tasks and powers which the Regulation reserves for the latter (Judgment of 4 July 2023, C-252/21, Meta Platforms and Others (Bundeskartellamt), paragraphs 43, 48 and 49). A fortiori, an authority which applies a national provision transposing the
ePrivacy Directive and does not adopt any measures based on the Regulation does not encroach upon the competence of the lead authority. The Authority is aware of the duty of loyal cooperation referred to by the Court in the same judgment, which concerns the authority called upon to apply the Regulation (paragraphs 52–54) and conduct that has already been the subject of a decision or an investigation by the competent authority (paragraphs 56–57 and 63): circumstances which do not apply in the present case.

In any event, it is hereby stated in advance that the Data Protection Authority will notify the DPC of this decision for any checks regarding jurisdiction that the Irish Authority itself may deem necessary.

3.5. Consent

Meta's argument. Meta contends that, in any event, authorisation within the operating system constitutes a positive action on the part of the user; that the consent thus expressed is free, specific, informed and unambiguous; that it relates to a single purpose and is revocable; and that the in-app setting is not a consent mechanism. This argument is put forward as a subsidiary argument to the main one concerning the inapplicability of Article 122 of the Code, emphasising that, even from this perspective, the processing carried out by the Company would be lawful. However, these arguments cannot be accepted.

The specificity of the request for authorisation. In this regard, as already set out above, the case file shows that the request for authorisation referred to by Meta does not meet the requirements of specificity and prior information: a user wishing to create a post, a story or a reel is directed to a screen stating that access to the gallery is used to 'share photos and videos, receive suggestions on which photos to upload and enable other features' (Technical Report, figs. 7–9; Meta, submission, §4.23.2, doc. 2), and, in a single step, to the system window requesting access to 'photos and videos'. This is a single request covering operations with different access requirements: posting a photo requires occasional, on-demand access limited to the selected content,

which, according to the Technical Report, can be achieved without system authorisations; the Feature, by its very nature, requires broad and continuous access to the gallery (Technical Report, para. 1.4).

From the perspective under consideration, it is also irrelevant that the user has the option, at system level and in relation to the entire Facebook app, to choose between the options 'Allow everything', 'Allow limited access' and 'Do not allow'. Firstly, this option was only introduced with the Android 14 update (autumn 2023), whilst up to and including Android 13, the 'Allow limited access' option was not available. Even where available, the option does not resolve the problem: access to the selected subset remains permanent unless explicitly revoked, and any change to the subset requires the authorisation procedure to be repeated, which effectively leads the user to grant the broadest possible authorisation (Technical Report, para. 1.4). Furthermore, it is reiterated that this choice made by the user relates to the entire Facebook app and does not refer to individual, specific features, as also confirmed by the Company.

Consequently, even the choice made by the user – when interacting with the system screens – is not specific to the Feature. Even if one were to assume that the user selected the 'Allow limited access' option, the infringement remains the same: in the Authority's view, the limited nature of the access makes no difference.

Meta's admissions. Indeed, the Company itself admits that the Feature "cannot operate on a 'one photo at a time' basis" (submission, §6.2) and that the system authorisation applies "to the App as a whole", whilst the ACCESS_MEDIA_LOCATION authorisation is stated "to be used by other and distinct functions of the App" (§5.35). Meta therefore confirms that the same authorisation request covers distinct and separate functions, and that this authorisation request cannot therefore fulfil the requirements of specific consent as mandated by the legislation, since the phrase "enable other functions" does not allow the user to understand which further processing operations it grants access to.

Meta refers to Recital 32 of the Regulation and Guidelines 5/2020 to argue that a single consent may cover multiple processing operations with the same purpose. It is therefore the Company itself that confirms that consent must be given separately for each purpose.

Freedom of consent. It must, however, be noted that, in accordance with recital 43 of the Regulation, consent cannot be deemed 'free' unless it is possible to give separate consent to distinct processing operations. Now, the publication of content chosen by the user and the scanning of the multimedia archive to suggest content for publication are operations that differ in nature, intensity and predictability: in the former, the user chooses the content; in the latter, it is Meta (via the app) that identifies and selects the content from amongst all that is accessible. Lumping both together under the same purpose of 'facilitating sharing' can only be done on the basis of the obvious vagueness of that purpose, which in itself is sufficient to render the requirement of specificity meaningless. Applying the same criterion, every function of a social network could be traced back to the purpose of 'sharing', which is the primary aim of anyone wishing to join a community. As noted in the Technical Report, the request for broad and continuous access should have been submitted at a different time and linked solely to the Feature, which is disabled by default (para. 1.4). In this regard, it should be emphasised that the Technical Report (para. 1.3) refers to the policy of Google LLC, the company that created and owns the Android operating system and is therefore the entity that defines its authorisation model and the rules that developers are required to comply with in order to distribute their apps through the relevant store, Google Play. For photo and video permissions, this policy stipulates that sensitive permissions must be requested incrementally, in the context in which they are needed, and that new consent must be obtained for additional purposes. The source is particularly significant: Google is the entity that devised the Android permissions model, to which Meta attributes the impossibility of requesting a permission for a single feature (storage, §6.1–6.3), and it is the same entity that, through its own policy, stipulates that sensitive permissions must be requested incrementally and within context. Meta cannot therefore invoke the Android model to justify a single request that the policy of its very creator advises against.

The requirement of specificity in European case law. European case law is unequivocal on the requirement of specificity. In particular, the Court has held that the expression of will must be 'specific', in the sense that 'it must relate precisely to the processing of the data concerned and cannot be inferred from an expression of will having a distinct purpose' (Planet49, paragraph 58; Orange România, paragraph 38). On the basis of this principle, it ruled out that clicking the button to enter a prize draw could suffice to regard consent to the installation of cookies as validly given (Planet49, paragraph 59), and asked the national court to ascertain whether the signing of a contract, which covered a number of clauses, could constitute specific consent to

one of them (Orange România, paragraph 47). The same reasoning applies in the present case: the general authorisation granted to publish a photograph cannot be construed as consent to broad and ongoing access to the archive for a separate purpose. As regards separate consent for distinct processing operations, referred to above in relation to recital 43, the Court has confirmed that consent is presumed not to have been freely given if it is not possible to give it separately for each processing operation (C- 252/21, Meta Platforms and Others, paragraph 144), and that users must be able to refuse
specific, unnecessary processing operations individually, without having to forgo the service as a whole (paragraphs 150–151). The very same Guidelines 5/2020 invoked by Meta, which permit a single consent for distinct processing operations only if these have 'the same purpose' (para. 57), also require granularity, that is, 'the possibility of giving separate consent for each purpose' (para. 60; see also para. 44), and specify that the purpose must be clearly defined as a safeguard against 'function creep', that is to say, 'the undue extension of functionality', which poses a risk to the data subject as it may result in 'a loss of control' over their data (paras. 55–56). As regards the specificity of the stated purpose, a vague or generic purpose, such as 'improving the user experience', does not meet the criteria for being 'specific' (Guidelines 5/2020, footnote 30, which refers to Opinion 3/2013 of the WP29 on purpose limitation).

The generic content of the system pop-up. It should also be noted that the system pop-up has generic content ('photos and videos') and the operating system is unaware of the processing operations the app intends to carry out: the user therefore remains unaware of the actual processing (Technical Report, para. 2). The fact that authorisation constitutes a positive action on the part of the user is not sufficient: in order to be equated with prior, free, specific, informed and unambiguous consent as required by the law, the positive action must relate specifically to the processing for which consent is sought.

Meta acknowledges that the in-app setting (i.e. the toggle switch in the Facebook app's settings under 'Get suggestions from your gallery when browsing Facebook') is not a consent mechanism (memorandum, §4.31). This setting merely activates or deactivates the Feature within the app and does not, in itself, grant any access to the gallery, which depends on the authorisation granted at operating system level. The operating system authorisation (the Android pop-up window requesting access to 'photos and videos') therefore remains the sole action taken by the user to grant access to the gallery. However, this authorisation is not specific to the Feature: it is requested from the user in order to post a photo or video, is granted 'to the App as a whole' and, as Meta acknowledges, also covers separate functions (storage, §5.35 and §6.2). A user who grants this authorisation to post content has therefore not expressed any intention specifically relating to the Feature. The consent thus expressed has, in fact, a different and more general subject matter – the app's access to 'photos and videos' – and cannot be extended to the Feature, since an expression of will 'cannot be inferred from an expression of will having a distinct subject matter' (Planet49, paragraph 58). It follows that the system-wide authorisation does not, with regard to the Feature, constitute the consent required by Article 122, which permits access 'only on condition' that such consent has been validly given. It is in these terms that the passage from Meta's defence must be examined, in which the Company, whilst not expressly invoking Article 122(2), argues that consent would be expressed through a device configuration. Even when understood in this way, the argument does not hold up: paragraph 2 permits consent to be given through settings that are easy and clear to use, but it still presupposes consent that meets the requirements of Article 122(1), namely that it is informed and specific, as well as free and unambiguous. The system dialogue box, which is generic by nature, does not allow consent with these characteristics to be given for the Feature. Furthermore, Guidelines 5/2020 specify, with regard to consent given through settings (in this example, those of the browser), that these must be designed in accordance with the conditions for the validity of consent, including the requirement that consent be granular for each of the intended purposes (para. 89), and that consent cannot be obtained through the same action by which a contract or general terms and conditions of service are accepted (para. 81) nor inferred from the mere continuation of normal use (para. 84).

The in-app setting is active prior to authorisation. It should also be noted that Meta admitted that the in-app setting could appear 'active' even before the user granted the system authorisation (recital, §4.33), contrary to what it had stated in its reply of 14 November 2025, where the option was 'inactive' for users who had not granted authorisation. Meta reports that it has resolved the issue with version 581 of the app, whilst specifying, however, that users who have not updated the app will continue to see the previous interface (memorandum, note 7).

The activation of the Feature without user choice. From another perspective, Meta maintains – and the Technical Report itself confirms – that the Feature does not operate until the user grants operating system

authorisation. The Authority takes note of this but draws a different conclusion from that of the Company. According to Meta's statement in its note of 14 November 2025, the in- app setting becomes active for users who have granted operating system authorisation: the Feature therefore launches when the user grants such authorisation – for example, to post a photo – without any further action being required and without the user ever having been asked to make a choice regarding it. The changes introduced with version 581 of the app (memory, §4.34) concern the consistency between the status displayed by the setting and the ability to access the feature, and not the moment at which the feature is activated. The consent required by Article 122 must result from a positive and unequivocal action by the user, not from silence or inactivity (Planet49; Orange România). Meta itself acknowledges that the in-app setting is not a mechanism for consent (submission, §4.31): it cannot therefore constitute, whether in the 'active' or 'inactive' state, the expression of will required by Article 122, and Meta cannot attribute to it the positive act required by the legislation. All that remains is the operating system authorisation, which the user grants for another purpose, typically the publication of content: the authorisation exists, but it does not relate to the Feature, in respect of which the user has not expressed any specific choice.

'Active behaviour' in case law. This principle is consistently upheld in case law. In particular, the Court has clarified that the requirement for an 'expression' of will 'clearly implies active, rather than passive, behaviour' (Planet49, paragraph 52) and that only active behaviour is capable of satisfying the requirement of unambiguity (paragraph 54). With regard to the pre-ticked box, it noted that it is 'practically impossible to determine objectively' whether the user has given their consent and whether they have done so in an informed manner, as it cannot be ruled out that they may not have read the information 'or even that they may not have seen that box at all' (Planet49, paragraph 55; Orange România, paragraph 37). Those principles, set out in relation to the pre-ticked box, apply all the more so to a function that is activated on the basis of authorisation granted for another purpose and which the user has never had the opportunity to choose or, in some cases, even to see.

The prior nature of consent. As regards the prior nature of consent, the current wording of Article 5(3) of the Directive requires that the data subject have "given his or her prior consent, having been informed in a clear and comprehensive manner […] inter alia of the purposes of the processing" (Planet49, paragraph 46; Court of Justice, judgment of 29 July 2019, C-40/17, Fashion ID, paragraphs 13 and 89). The Court of Justice has clarified that this wording is the result of a deliberate choice by the European legislator: the initial version of the provision merely provided for the 'possibility of refusing' the installation of cookies, whereas Directive 2009/136/EC replaced those terms with 'has given his or her prior express consent', so that the user's consent 'can no longer be presumed and must result from the user's active behaviour' (Planet49, paragraph 56). In the same vein, the Court has held that consent must be given prior to the operation and that information must be provided 'immediately, that is to say, at the time of collection', in order to ensure 'effective and timely protection of the data subject's rights' (Fashion ID, paragraphs 102 and 104, referring to Directive 95/46). The sequence is the same in the Italian text, which permits access to information already stored "only on condition that" the user has given their consent after being informed: first the information, then the consent, then the access. The EDPB also considers that the preventive nature of consent is "clearly implicit" in the definition set out in the Regulation, in that consent must be given before the processing activity takes place (Guidelines 5/2020, para. 90). It follows that authorisation must be prior and active, and cannot be inferred from passive behaviour, nor from an act carried out for a different purpose.

Existing users and the absence of new notifications. Furthermore, the Technical Report noted that users who were already using the app at the time of the update to Android 13, and who had the previous READ_EXTERNAL_STORAGE authorisation, automatically received the READ_MEDIA authorisations. Meta reports that the warning preceding the permission request appears only to users who have not yet granted the permission (memorandum, §5.32.2) and acknowledges that no further, separate notification was sent (§5.31). Users who had already granted the permission prior to the launch of the Feature in 2023 therefore never received a request relating to it, nor did they have the opportunity to express a related preference, as the only action attributable to them was the permission granted previously, for other purposes and before the introduction of the Feature.

The revocability of consent. Meta also points out that consent is revocable (submission, §4.24) and that revocable access cannot be defined as 'continuous'. The Authority observes that revocability relates to the possibility of withdrawing consent (Article 7(3) of the Regulation), not to the validity of the consent at the time it is given; and that continuity is a characteristic of the access that the app may carry out until the

authorisation is revoked, not of the impossibility of revocation. The Technical Report notes, moreover, that in most cases authorisation, once granted, remains permanent until the user revokes it of their own accord, and that revocation requires an explicit and informed action within the system settings, although the user may make use of the summary screen provided by the app (paragraph 1.1 and note 3). Moreover, the argument regarding the difficulty of withdrawing consent is not among the grounds on which this decision and the preliminary complaint are based.
The burden of proof regarding consent. As regards the burden of proof, the Court has clarified that it is for the data controller to demonstrate the existence of valid consent (Orange România, paragraphs 42 and 51–52; C-252/21, Meta Platforms and Others, paragraphs 95 and 152; Guidelines 5/2020, paras. 104–107), that it cannot expect users to actively express their refusal (Orange România, para. 51) and that the mere performance of an act, such as signing a contract containing a clause, does not in itself demonstrate consent 'in the absence of indications confirming that that clause has actually been read and understood' (Orange România, paragraph 46). In the present case, Meta has not produced any evidence to show that users, when granting the system authorisation, understood that this would enable the Feature; and for those users who, having received the update to Android 13, were already using the Facebook app and that app already had the previous READ_EXTERNAL_STORAGE authorisation, this authorisation was automatically extended to include READ_MEDIA authorisations, as there was no new act of will expressly relating to access to the gallery, let alone to the Feature.

In this context, therefore, the consent required by Article 122(1) and (2) of the Code was not validly obtained.

3.6. The strict necessity and the legal grounds invoked

The strict necessity invoked by Meta. In its subsidiary arguments, Meta asserts that access is strictly necessary for the provision of a service explicitly requested by the user, consisting of the 'efficient and effective process of uploading photographs' (submission, §4.37). This argument, set out in a single paragraph and without any supporting evidence, is unfounded. The exception to consent under Article 122(1) must be interpreted restrictively and concerns access that is strictly necessary to provide a service that the user has explicitly requested.

In fact, the Feature is not a service requested by the user but, as Meta states, "an optional tool within the App" (submission, §2.2), which can be disabled (§1.3.6). The service actually requested by the user – namely, the publication of content – can be provided even without the Feature being active and with access limited to the selected content, as demonstrated by the existence of the 'photo picker' function; Meta acknowledges, in fact, that the Feature requires access different from that necessary to publish individual photos (statement, §6.2–6.3). The Authority did not consider the 'photo picker' to constitute an obligation, nor does it treat it as a separate charge, as Meta observes (§6.1): this technical observation is valuable as a factual element, which excludes the strict necessity of general access to the archive for the Feature and confirms the distinct nature of the processing operations.

The restrictive interpretation of grounds for processing other than consent. The rigour with which the Court interprets grounds for processing other than consent confirms this conclusion. Even with reference to Article 6 of the Regulation, the Court has noted that the grounds rendering processing lawful in the absence of consent must be interpreted restrictively (C-252/21, Meta Platforms and Others, paragraph 93); that the requirement presupposes processing that is 'objectively indispensable' for the fulfilment of a purpose that is an integral part of the service provided to the data subject, and that the controller must be able to demonstrate how the main subject matter of the contract could not be achieved without the processing (paragraph 98); that the fact that the processing is 'merely useful' is irrelevant and that 'there must be no other viable and less intrusive alternatives' (paragraph 99); and that, if the contract comprises several distinct elements of the same service, the assessment must be carried out separately for each one (paragraph 100). Applied by analogy, these criteria preclude general access to the archive from being deemed strictly necessary for an upload that can be made more 'efficient' but is achievable using less intrusive means; and the burden of proving the contrary lies with Meta, which has failed to do so.

The legal bases invoked by Meta. As regards the legal bases invoked, the Authority agrees with Meta's assertion that Article 122 of the Code and Article 6 of the Regulation operate on distinct levels. It follows that access to information stored on the terminal cannot be justified on the grounds of legitimate interest nor, except where strictly necessary, on the grounds of contractual necessity, whatever legal bases Meta may

intend to invoke for the subsequent processing. Contrary to Meta's assertion, the opening notice did not confuse the two levels: it noted that, in responding to the Authority's request regarding the legal basis and the consent mechanism (questions 3 and 4 of the request of 27 October 2025), Meta had cited the contract and legitimate interest, which are not sufficient to legitimise access under Article 122. In its written submission, Meta clarifies that, for the purposes of access, it relies solely on the consent expressed through the system authorisation and, in the alternative, on strict necessity: both grounds have been rejected.

The distinction between the two approaches, and its consequences, is reflected in EDPB Opinion 5/2019. Since Article 5(3) of the Directive provides for prior consent as the rule, it—insofar as the information stored on the terminal constitutes personal data—"takes precedence over Article 6 of the
General Data Protection Regulation with regard to the storage of or access to such information', and the controller 'cannot rely on the full range of grounds for lawfulness set out in Article 6' (Opinion 5/2019, para. 40). The contract and legitimate interest cited by Meta cannot therefore justify access linked to the Feature. They may, if anything, be relevant to prior and subsequent processing operations, which are not governed by a specific provision of the Directive and remain within the remit of the lead authority (Opinion 5/2019, para. 75), and which this decision does not examine. In the same vein, the Court of Justice considered it relevant to examine Article 7(f) of Directive 95/46 solely because the data transmitted 'are not necessarily limited to information stored on the terminal equipment' (Fashion ID, paragraph 91).

The choice of legal bases on the basis of age. The Authority does not comment on the point raised in the notice of initiation, namely that the use of two different legal bases depending on the user's age reflects a 'choice of convenience', which relates to the processing operations governed by the Regulation and to the competence of the lead authority (paragraph 3.4). However, it cannot fail to observe that this choice falls within the category of formalistic solutions lacking any real legal substance, which present a contradictory and intrinsically weak picture of the fundamental choices made by the data controller with regard to the processing operations in question.

3.7. Information to users (Article 122(1) of the Code)

In this regard, Article 122(1) requires that the user be informed before giving consent. The information provided by Meta is deficient in four respects.

Existing users. In this regard, the notice initiating the proceedings noted that users who were already active at the time the Feature was introduced did not receive any information. Meta does not dispute this: it merely observes that 'no additional and separate notification was required' (statement of defence, §5.31) and to cite, as transparency tools (§5.32), the general privacy notice, the notice preceding the authorisation request and the sharing suggestion. However, these are tools that do not reach users who had already granted authorisation prior to 2023. The notice, in fact, is only displayed to those who have not yet granted authorisation. The sharing prompt appears when the Feature is already operational and the processing is already underway; consequently, by definition, it cannot constitute prior information. Finally, the general privacy notice is a document which the user cannot be expected to review after every app update and which, as already noted, does not specifically describe the Feature. Nor can the argument that the data is 'non-sensitive' and the processing 'consistent with the app's main functions' (§5.30) serve to justify the omission: prior information is a condition for the validity of consent, and it is Meta's responsibility to demonstrate that it has provided this to users, regardless of the nature of the data processed and the degree to which the processing is foreseeable to the user.

The wording of the privacy notice. It should also be noted that the wording Meta cites as a reference to the Feature ("remind you when you have new photos to upload") does not identify the Feature or describe how it works: it does not explain that the app autonomously selects content from the gallery to suggest to the user that they publish it. This wording, which Meta itself states has been included in the privacy notice since July 2022 (statement of defence, §5.37), predates the launch of the Feature, which, according to Meta, took place in 2023 (note of 14 November 2025): the privacy notice was therefore not updated at the time of the launch. The opening statement also noted that the privacy notice contains no specific information on the Feature, and that the closest wording ("Content you provide via our camera features, your gallery settings or voice features") appears twenty-three times in the text, including in connection with purposes such as the personalisation of adverts, which are not apparent from the information provided within the product; the response makes no comment on this point. Meta refers to the Article 29 Working Party's Transparency

Guidelines, according to which the data controller must strike a balance between completeness and conciseness. The Authority does not consider that the privacy notice must describe every function of an app, but that the information necessary to decide whether to consent to a particularly intrusive form of processing (accessing the user's photo library is clearly such a form) must be provided specifically at the time consent is requested.

The notice preceding the request for authorisation. The notice preceding the request for authorisation lists, amongst the purposes, that of 'enabling other functions': a generic phrase which does not allow the user to understand what processing they are actually granting access to. Furthermore, the notice does not distinguish between the publication of individual photos – which requires occasional and limited access to the selected content – and the Feature, which instead requires broad and continuous access to the entire gallery (where the user selects the 'Allow all' option, as the system's request prompts them to do). Nor does it clarify that, once granted, the authorisation enables the app to access all photos and videos on the device and that it remains valid for every function, not just the one for which it was requested. As for the settings screen, Meta acknowledges that the option could appear to be active even before authorisation was granted (record, §4.33): as a result, the user was presented with information that did not reflect the actual situation. The Authority takes note of the changes introduced with version 581 of the app, the Help Centre article published in April 2026 and the further updates announced. However, these measures were taken after the complaint was lodged (July 2025) and the Authority's request for information (October 2025), and they concern only users who update the app; they cannot remedy the unlawfulness of access that had already taken place. The Authority takes this into account solely for the purposes of quantifying the fine (para. 6.2).

The content of the information required. As regards the content of the information required, the Court has clarified that 'clear and comprehensive' information implies that the user is able to 'easily determine the consequences of any consent given' and to give such consent 'in full knowledge of the facts', and that the information must be 'clearly understandable and sufficiently detailed' (Planet49, paragraph 74; see also Orange România, paragraphs 40 and 52, according to which the information must be provided in advance, in a comprehensible and easily accessible form, and in plain and simple language). In the same judgment, the Court included the duration of the cookies' activity within the information required, because a long or unlimited period implies the collection of a large amount of information (Planet49, paragraphs 75 and 78), as well as the possibility of access by third parties (paragraphs 75 and 80). By analogy, the duration of the access granted through system authorisation, its extension to the entire database (in the form of 'Allow all') and its validity for functions other than that for which it is requested, are essential pieces of information for assessing the consequences of the choice and are precisely those which are missing from Meta's notice. This finding remains unchanged even if the user can opt for limited access: even in that case, the notice fails to make clear the duration of the access and its validity for every function of the app, and the limited nature of the access makes no difference as regards the lack of information. As regards the timing of the information, which must be provided immediately (Fashion ID, paragraph 104, already referred to in section 3.5), it cannot be deferred to general documents or to a later date. Guidelines 5/2020 specify, as the minimum information required for informed consent, the identity of the data controller, the purpose of each processing operation for which consent is sought, and the types of data that will be collected and used (paragraph 64), to be provided specifically for each request for consent (paragraph 61); these requirements are not met by Meta's notice, which refers generically to 'enabling other features'.

Overall, the user was not in a position to understand, before granting access, that they would be enabling Meta to systematically scan their photo library in order to suggest content for publication. The information therefore fails to meet the requirement of Article 122(1), which stipulates that the user must be informed 'by means that ensure effective awareness'.

3.8. Further aspects and scope of the subjective element of the infringement

For the sake of completeness and in response to the Company's submissions, the Authority clarifies that Meta's liability cannot be inferred from the following aspects, even though they emerged during the preliminary investigation:

− the Technical Report, and consequently the notice of initiation, merely state that the complexity of the settings screens 'could constitute' an obstacle and that certain elements 'could constitute' misleading design patterns within the meaning of EDPB Guidelines 3/2022. Meta notes that these formulations are

precautionary (statement of defence, §5.45). The Authority therefore does not derive a separate charge from them and considers them, within the limits indicated above, solely as context for the inadequacy of the information;

− the name of the Feature, which the various formulations used in the app (‘suggestions to share from your gallery’, ‘get suggestions from your gallery when browsing Facebook’, ‘suggestions on photos to upload’) could render ambiguous; this observation, expressed in hypothetical terms, does not form the basis of the decision;

− the ACCESS_MEDIA_LOCATION authorisation is declared in the Manifest and, according to the Technical Report, it is ‘highly likely’ that it is granted via the same system authorisation window as that for photos, although it is not possible to verify this. Meta states that the Feature does not use it and that it is declared at application level for other functions (storage, §5.34– 5.36). The Authority does not establish that the Feature accesses location data, but notes that Meta acknowledges that the same authorisation request covers functions other than the one under consideration;

− the use of content for training artificial intelligence, which Meta has denied in relation to unpublished content and which the Authority is unable to verify, given the absence of the app’s source code and the encryption of traffic, meaning that verification would have required the full cooperation of the data controller. Meta stated, in its response of 14 November 2025, that the Feature does not use generative artificial intelligence and that it does not intend to use unpublished content from the gallery to develop and improve its AI, which would be fed solely by content that adult users make public or share with Meta AI as part of a prompt, unless they object. In its written submission (§2.2), it reiterated that the Feature does not involve generative AI or cloud processing and does not entail analysis of the content of photos or videos. In the same submission, however, in a footnote (footnote 4, in §1.3.6), the Company clarified that the same settings page contains a further, separate feature, called ‘Get creative ideas tailored to you by enabling cloud processing of your photo gallery’, presented as a ‘New Feature’, launched in the European Union in early 2026 following consultation with the DPC, which is not the subject of these proceedings. This raises questions which the Authority cannot resolve at this stage of the proceedings: the new feature, by its very name, involves the processing of photo gallery content in Meta’s cloud, which is precisely what Meta excludes for the feature under consideration;

since, according to the company itself, the operating system authorisation applies to the app as a whole (memorandum, §6.1–6.3), it could be based on the authorisation already granted by users; it is unclear whether, and in what manner, users are informed of this and consent to it; and Meta’s denial regarding training is limited to ‘unpublished’ content and is phrased in prospective terms (‘does not intend’), so it does not clarify whether the content processed in the cloud, or its derivatives, is or may be reused to develop and improve the AI. These issues do not form the basis of this decision, but the Authority reserves the right to carry out separate investigations into the new feature, including through requests for information (Article 157 of the Code) and access, inspections and audits (Article 158 of the Code), with regard to the legal basis, user information and consent, the reuse of content for model training and the relationship with the system authorisation already granted, as well as to assess coordination with the DPC on matters falling within its respective remit. Article 122 does not require such an assessment for the purposes of establishing unlawfulness.

The scope of the infringement. As regards the scope of the infringement, Meta disputes the estimate of approximately 20 million users, without, however, providing any alternative figure, even though the notice of initiation had required it to indicate any information relevant for the purposes of Article 83(2) of the Regulation. As was the case with the app’s system architecture, Meta did not consider it necessary to provide any clarification regarding the scope of the Feature, despite being the only party in a position to know the relevant data (the number of Italian users on Android devices who had granted the operating system authorisation). What Meta should have provided, in the spirit of loyal cooperation with the Authority, was therefore reconstructed by the Authority itself on the basis of public and reliable sources. According to AGCOM’s Communications Observatory Report No. 4/2025 (paragraph 2.15, p. 28), compiled using Audicom–Audiweb data, there were 35.6 million monthly unique Facebook users in Italy in September 2025. According to figures based on Meta’s advertising resources, as reported by DataReportal (Digital 2026: Italy), Facebook’s audience in Italy stood at approximately 28.5 million users at the end of 2025. Given that, according to Statcounter’s findings, the Android system accounts for approximately 63 per cent of mobile

usage in Italy, applying this proportion to the two figures results in an audience of between approximately 18 and 22 million users, which confirms the estimate of approximately 20 million contained in the notice of proceedings. It should also be noted that the exact figure is not a constituent element of the infringement and does not affect the assessment; as regards the penalty, the Authority takes this into account within the limits of the uncertainty arising from the Company's failure to cooperate, which cannot therefore work in its favour.

3.9. Subjective element

The infringement was committed with significant negligence. Meta is, in fact, a global operator with specialised compliance structures and is aware of how Android's authorisation model works and of competitors' policies regarding access to photos and videos, which provide for incremental requests, in context, and new consents for further purposes. In particular, the decision to combine functions with different access requirements into a single request, whilst presetting the Feature as active, is a design choice made by the Company and not an unavoidable consequence of the operating system, as the Technical Report has demonstrated. Furthermore, in its reply of 14 November 2025, the Company provided the Authority with inaccurate information regarding the status of the setting for users who had not granted authorisation; this was only rectified in its defence submission. The subsequent measures do not preclude liability and are taken into account for the purposes of the penalty (paragraph 6.2)

4. CONCLUSIONS

In light of these considerations, the allegations set out in the notice initiating proceedings under Article 166 of the Code are confirmed, within the limits specified in paragraphs 3.4 and 3.8, as the statements made and the documentation produced during the preliminary investigation are not sufficient to rebut the findings made by the Authority, and none of the cases provided for in Article 11 of Regulation No 1/2019 apply.

Consequently, the Authority finds that the conduct of Meta Platforms Ireland Limited was unlawful, in that it accessed, via the Facebook app for Android devices, information stored on the devices of Italian users (photographs, videos and related metadata) via the Facebook app for Android devices for the 'Get suggestions from your gallery when browsing Facebook' feature, without having obtained specific and informed consent for that feature – distinct from that relating to the app's other features – and without having informed users in advance in a manner sufficient to ensure their effective awareness, in breach of Article 122(1) and (2) of the Code. No separate infringements of Articles 6, 7, 12 and 13 of the Regulation have been established, which are referred to as substantive criteria in accordance with paragraph 3.4.

It should also be noted that the infringement established in accordance with the grounds set out above cannot in any way be considered 'minor', given the number of data subjects potentially affected (approximately 20 million Android users in Italy), the duration (from 2023, according to Meta's statement, and still ongoing for users who have not updated the app), the structural nature of the design choice, and the size and economic capacity of the data controller (see recital 148 of the Regulation).

5. REMEDIAL MEASURES

It should first be noted that the conduct has not ceased. The changes introduced with version 581 of the app, as stated by Meta, apply only to users who update the app; others continue to see the previous interface (see footnote 7), nor has Meta stated that it has requested new consent from Italian users who had already granted system authorisation. The declared rectification (Help Centre article, version 581, updates in preparation) is not verifiable and does not address the mechanism for obtaining consent; nor is it accompanied by the technical evidence which the Authority, for systems of this type, can obtain only through the cooperation of the data controller (see below, paragraph 6.2). It therefore appears necessary to impose the following corrective measures on Meta, proportionate to the size and technical capacity of the company:

− pursuant to Article 58(2)(d) of the Regulation, Meta is ordered to bring its processing operations into compliance, within sixty days of notification, by adopting the following measures in respect of Italian Facebook users on Android devices:

(i) to obtain consent for access to the gallery for the Feature by means of a separate and specific request, not combined with the request for authorisation to publish photos and videos or with other functions, and without

generic phrases such as ‘enable other functions’;
(ii) inform the user, at the time of the request, in a clear and comprehensible manner, of the purpose of the Feature, the fact that it involves access to the media library, and how to disable it and withdraw authorisation;
(iii) keep the Feature disabled by default and enable it only following an explicit expression of consent by the user in relation to it;
(iv) obtain consent in this manner even from users who have already granted system-wide authorisation, keeping the Feature disabled until such consent is given;
(v) ensure that the setting status corresponds to the actual processing status for all versions of the app in use in Italy, including through server-side checks or mandatory updates;

− pursuant to Article 58(2)(f) of the Regulation, prohibits Meta, once the sixty-day period referred to in the previous point has elapsed without action, from making the Feature operational for Italian Facebook users on Android devices who have not given their consent in the manner specified, until compliance is achieved; it also prohibits Meta from processing any information processed via the Feature in the absence of consent obtained in accordance with the specified procedures;

− pursuant to Article 58(1)(a) of the Regulation and Article 157 of the Code, orders Meta to inform the Authority within thirty days of the measures taken, including for the purposes of resolving the dispute in accordance with Article 166(8) of the Code, and, within ninety days of notification, the solutions adopted to implement the measures set out above, attaching the relevant technical documentation (including screenshots of the new interfaces and statements on the functioning of the processing, indicating whether the information in the gallery, including derived information, is transmitted to Meta’s systems prior to publication), as well as the number of Italian users on Android devices who have given their consent in accordance with the new procedures.

6. ORDER-INJUNCTION

Pursuant to Article 58(2)(i) of the Regulation and Article 166 of the Code, the Data Protection Authority has the power to impose an administrative fine pursuant to Article 83 of the Regulation, by issuing an injunction (see Articles 18, Law No. 689 of 24 November 1981, and Article 16(1) of the Data Protection Authority’s Regulation No. 1/2019).

6.1. Assessment of the conduct and determination of the applicable penalty

The breach of Article 122 of the Code is subject to the penalty provided for in Article 83(5) of the Regulation, pursuant to Article 166(2) of the Code. Since a breach of a single provision has been established, resulting from a single act (the design and operation of the Feature with the access mechanism described), Article 83(3) of the Regulation does not apply.

For the purposes of quantifying the fine, it is first necessary to identify the maximum statutory limit, which is 20 million euros or, if higher, 4 per cent of the total annual worldwide turnover for the preceding financial year (Article 83(5) of the Regulation). In this regard, the dynamic ceiling takes precedence over the static ceiling where the undertaking’s turnover exceeds 500 million euros (European Data Protection Board, ‘Guidelines 4/2022 on the calculation of administrative fines under the GDPR’, version 2.1 adopted on 24 May 2023, hereinafter ‘Guidelines 4/2022’, paras. 114–116).
The concept of an undertaking. In this regard, it should be noted that the relevant parameter is not the turnover of the company to which the measure is addressed alone. Indeed, Article 83(4)-(6) of the Regulation, in the light of recital 150, refers to the concept of ‘undertaking’ in Articles 101 and 102 TFEU, which designates an economic unit even if it consists of several legal persons: where the data controller forms part of an undertaking as defined above, the dynamic upper limit is calculated on the basis of the turnover of the undertaking as a whole (Guidelines 4/2022, paragraphs 118–122; Court of Justice, judgment of 5 December 2023, C-807/21, Deutsche Wohnen, paragraphs 53–59). From another perspective, if the parent company holds all or almost all of the subsidiary’s share capital, it is presumed to exercise a decisive influence over it, unless the contrary is proved (the so- called ‘Akzo presumption’; Court of Justice, judgment of 10 September 2009, C-97/08 P, Akzo
Nobel, paragraphs 60–61; Guidelines 4/2022, paras. 124–125). In the present case, Meta Platforms Ireland Limited has produced its annual accounts as at 31 December 2024, certified on 30 July
2025, which show that its ultimate parent company is Meta Platforms, Inc. The records of the Media

Ownership Ireland project (an initiative of Coimisiún na Meán and the DCU School of Communications; data updated to December 2025, consulted on 25 October 2026 and included in the case file) also reveal a wholly controlling chain of ownership: Meta Platforms Ireland Limited (no. 462932) is wholly owned by Facebook International Operations Limited (no. 514293), which in turn is wholly owned by Facebook Ireland Holdings Unlimited Company (no. 466405), the share capital of which is wholly held by Meta Platforms, Inc. Meta Platforms, Inc.'s Form 10-K for the financial years ended 31 December 2024 and 2025, filed with the Securities and Exchange Commission (Annex 21.1, list of subsidiaries), includes Meta Platforms Ireland Limited amongst the subsidiaries of Meta Platforms, Inc., consistent with the information set out in the financial statements provided. The list contains no indication of a shareholding of less than 100 per cent of the company's share capital, nor of any other shareholders, and therefore confirms, in the absence of any contrary specification, the picture of total control emerging from the registers referred to above. The full ownership throughout the entire chain, which is headed by Meta Platforms, Inc., therefore gives rise to the presumption that the parent company exercises decisive influence, and Meta has not provided sufficient evidence to rebut this presumption. The reference entity is therefore the group headed by Meta Platforms, Inc., whose turnover is derived from the consolidated financial statements (Guidelines 4/2022, paragraphs 128–130).

The relevant financial data. As regards the relevant financial data, the consolidated financial statements of Meta Platforms, Inc. (Form 10-K, accession no. 0001628280-26-003942, Item 8, 'Consolidated Statements of Income') for the financial year ended 31 December 2025 – the most recent financial year for which accounts had been finalised and published at the date of this decision – show revenue of US$200,966 million and a net profit of US$60,458 million. It should also be noted that the relevant turnover is that of the financial year preceding the decision imposing the penalty (Guidelines 4/2022, para. 131). That being said, applying the reference exchange rate published by the European Central Bank for 31 December 2025, the financial year-end (1 euro = 1.1750 US dollars; Official Journal of the European Union, Series C, C/2026/44 of 5 January 2026), the turnover amounts to approximately 171,035 million euros (171,034,893,617 euros) and net profit at approximately 51,454 million euros. The dynamic ceiling, equal to 4 per cent of turnover, is therefore approximately 6,841 million euros (6,841,395,745 euros), which is significantly higher than the static ceiling of 20 million euros, which is not relevant.

Finally, it should be noted that the ceiling is not commensurate with the turnover generated in Italy nor with the scope of the infringement: the Regulation links it to the economic scale of the undertaking as a whole, whilst the national nature of the infringement and the number of users involved are relevant for the purposes of determining its gravity (paragraph 6.2).

6.2. Determination of the administrative fine (Article 83(2) of the Regulation)

The amount of the administrative fine must be determined on a case-by-case basis, taking due account of the factors set out in Article 83(2) of the Regulation.

To this end, the Authority follows, for the purposes of transparency and consistency, the methodology set out by the EDPB in Guidelines 4/2022, which involves identifying the starting point (classification of the infringement, gravity, the undertaking's turnover), the assessment of aggravating and mitigating circumstances, and the final verification of effectiveness, proportionality and dissuasiveness, without this amounting to a purely arithmetic calculation; the calculation must always be based on an assessment of all the circumstances of the case (paragraph 145). Furthermore,
each criterion in Article 83(2) is taken into account only once (paragraphs 72 and 133) and the size of the undertaking is not counted twice (paragraph 64).

Seriousness of the infringement. For the purposes of quantification, the starting point is the seriousness of the infringement in the specific case, assessed in the light of the nature, gravity and duration of the infringement (Article 83(2)(a)), whether it was intentional or negligent (point (b)) and the categories of data concerned (point (g)), considered as a whole (Guidelines 4/2022, paras. 51–52 and 59). The breach falls, first and foremost, within the category for which Article 83(5) provides the highest maximum fine, which reflects the greatest severity in the abstract (paras. 49– 50). In the specific case, the following elements are relevant:

− nature of the infringement: Article 122 protects the integrity of the user's private life and their right to self-determination regarding access to the terminal; the infringement concerned the very basis of that protection,

namely prior, specific and informed consent, which was never sought for the Feature, thereby effectively undermining the purpose of the provision (Guidelines 4/2022, para. 53(a)). The context is that of commercial processing carried out by an operator in a position of significant information asymmetry vis-à-vis users, through a closed and unverifiable system, in relation to which the Authority requires the fullest possible cooperation from the data controller (see paragraph 3.3), relating to an archive that may contain images of minors or otherwise sensitive material, the presence of which is potential and not confirmed (paragraph 53(b)(i));

− subject matter of the processing and number of data subjects: the breach is nationwide in scope and concerns the multimedia archive of users who have granted authorisation, either in full or in a limited form, via an app used on a daily basis; the number of people affected is in the region of twenty million Android users in Italy, according to the estimate in the case file, which Meta has not refuted with its own data despite being requested to do so, and represents a considerable proportion of the resident population; this figure also includes users who have never used the Feature, which gives the breach a systemic nature (paragraph 53(b)(ii) and (iv));

− purpose of the processing: the Feature is designed to increase the use and sharing of content on the platform, which is the company's core business; the more central the processing is to the controller's core activities, the more serious the infringements are (para. 53(b), iii)). This factor is assessed here and is not counted again as a circumstance under Article 83(2)(k);

− duration: according to Meta, the Feature was introduced in 2023 and the conduct is still ongoing for users who have not updated the app and for those who have already granted system authorisation, meaning that the infringement has continued for several years (paragraph 53(c));

− level of harm: no concrete and individual harm has been proven, and the Authority has not established any transfers, further uses or processing of special categories of data; it does, however, note the potential, non-marginal harm arising from the user's loss of control over access to a repository of private content, which the Regulation takes into account even where the harm 'may have been suffered' and does not require proof for the purposes of the penalty (paragraph 53(b)(v)). In this regard, the Court of Justice has recognised, albeit in the different context of the balancing test under Article 6(1)(f) of the Regulation, that very extensive processing which significantly affects the user 'may give rise to a feeling of constant surveillance of their private life' (judgment of 4 July 2023, C-252/21, Meta Platforms and Others, paragraph 118; see also paragraphs 112 and 117 on the user's reasonable expectations). In practice, this factor carries limited weight;

− intentional or negligent conduct (Article 83(2)(b)): the infringement is negligent, as no intention to circumvent the rule has been established; however, the negligence is not minor, as this concerns a global operator, fully aware of the rules and the operating system's authorisation model (see paragraph 3.9), which could have avoided design choices such as the a single authorisation request covering multiple functions, the pre-setting of the Feature as active, and generic information; negligence does not equate to unintentional conduct, and the degree of negligence may be relevant (paragraphs 55–56);

− categories of data (Article 83(2)(g)): photographs, videos and metadata (date and time, type, orientation) are common data, and no use of location data or special categories of data has been established; however, the authorisation, in the form of 'Allow all' which the system prompt leads users to grant, enables access to the entire archive, and the volume of data relating to each data subject exacerbates the infringement of privacy (para. 58), all the more so as the archive may contain information of a particularly sensitive nature (para. 57). The Court of Justice has also noted that, in the case of data capable of revealing special categories of information, the risk to fundamental rights exists 'irrespective of their stated purpose' and of whether the data controller acts with the intention of obtaining such data (C-252/21, paragraphs 69–70), without this constituting a prerequisite for the assessment.

Taken as a whole, these factors (national and systemic scope, duration, centrality to the core business, volume of accessible data, and a degree of fault that is not minor), in the absence of any established actual damage, intent, confirmed data transfers or special categories of data, lead to the conclusion that the level of seriousness of the breach is moderate (Guidelines 4/2022, para. 60), at the lower end of the scale.

Initial amount. That said, for cases of medium gravity, the initial amount ranges from 10 per cent to 20 per

cent of the applicable upper limit (paragraph 60). In this regard, as the undertaking's turnover far exceeds 500 million euros, no size-based adjustment to the initial amount applies, because the size of the undertaking is already reflected in the dynamic ceiling (paragraph 66, last subparagraph). Applying this band to the ceiling of €6,841,395,745, the initial amount ranges from approximately €684.1 million to approximately €1,368.3 million. It should also be noted that the bands are not fixed amounts and that the Authority may utilise the entire range, up to the statutory ceiling, to tailor the fine to the circumstances of the case (paragraphs 47 and 69). In light of the factors assessed above, in particular the absence of intent, of established actual damage, of established data transfers and of special categories of data – which only partially offset the factors pointing in the opposite direction – the initial amount is set at 10.2 per cent of the statutory maximum, amounting to 700,000,000 euros.

As regards aggravating and mitigating circumstances (Guidelines 4/2022, Chapter 5), each of which is considered only once and without repeating factors already assessed for the purposes of determining the seriousness of the infringement (paragraph 72), it is considered that the following should be taken into account:

− Following the Authority's notification and request, Meta introduced version 581 of the app, with a setting that cannot be activated without system authorisation; in April 2026, it published an article on the Help Centre and announced further updates; this constitutes a mitigating circumstance of moderate weight, as it was belated, applies only to users who update the app, and has no bearing on the consent-gathering mechanism or on users who had already granted authorisation (see Article 83(2)(c) of the Regulation (Guidelines 4/2022, paragraphs 75–76, according to which measures implemented after the investigation has commenced are treated differently, as mitigating factors, compared to those taken voluntarily);

− Meta determines the architecture of the app and the mechanism for requesting authorisations and has full control over them; there is no evidence that it has taken measures to separate the
request for access to the Feature from that for publication (see Article 83(2)(d) of the Regulation;
Guidelines 4/2022, paragraphs 77 and 81). This factor has a moderate aggravating effect, given the higher level of responsibility provided for in the Regulation (paragraph 81);

− In the absence of specific final findings regarding this Feature, no account is taken of the pending regulatory proceedings referred to in the notes to the financial statements submitted (see Article 83(2)(e) of the Regulation); as regards previous cases, the Data Protection Authority's injunction order No 134 of 14 June 2019 (web doc. No. 9121486, hereinafter 'Order No. 134/2019'), by which a fine of EUR 1,000,000 was imposed on Facebook Ireland Ltd, now Meta Platforms Ireland Limited, jointly and severally with Facebook Italy S.r.l., pursuant to Article 164-bis, paragraph 2, of the Code (in its previous version) for breaches of Articles 13 and 23 of the Code, in relation to the disclosure of the data of 214,077 Italian users on the basis of a generic privacy notice and non-specific consent, with pre-selected settings and no alternatives for the user. This is a breach that had already been established prior to this decision, committed by the same data controller, concerning a similar matter and in any event carried out in a similar manner (Guidelines 4/2022, paragraphs 82 and 87–92). The time that has elapsed and the different regulatory framework in force at the time mitigate the severity of the infringement (paragraphs 84–86 and 91), without ruling it out, as there are no limitation periods (paragraph 85). This factor therefore constitutes a slight aggravating circumstance (paragraph 94);

− Meta responded to the Authority's requests, exercised its right of access and submitted a detailed statement; however, its overall conduct does not comply with the duty of cooperation incumbent upon the data controller. The Company, in fact, presented as 'voluntary' a form of cooperation that is in fact required by law, and the making of false statements in this regard is punishable under Article 168 of the Code; in its reply of 14 November 2025, it provided inaccurate information regarding the status of the configuration, which was only rectified in its defence submission; it did not accompany its statements with any technical evidence to support them, even though the Facebook app is closed-source software with encrypted traffic, in respect of which the Authority cannot do without the full cooperation of the data controller, who alone is able to provide the data and evidence necessary to reconstruct the actual functioning of the Feature; and failed to specify the number of users who had granted authorisation, as well as the other data required for the purposes of Article 83(2), thereby making it more difficult to assess the extent of the infringement. Such an attitude, which has placed the burden on the Authority to reconstruct facts falling within the exclusive knowledge of the Company, does not reflect the level of cooperation expected of an operator of such size and standing, and has

in no way contributed to limiting or avoiding adverse effects on users' rights. The level of cooperation must therefore be regarded as poor and constitutes a significantly aggravating circumstance (Article 83(2)(f) of the Regulation; Guidelines 4/2022, paragraphs 96–97;

− the Authority became aware of the facts through a report from a consumer association and not on Meta's own initiative (see Article 83(2)(h) of the Regulation), a neutral factor, as no spontaneous notification can be identified (Guidelines 4/2022, paragraphs 98–99);

− according to Meta, the Feature is designed to encourage the sharing of content on the platform; the business of Meta Platforms Ireland Limited consists, according to the notes to the financial statements, of invoicing for advertising products on Facebook and the group's other services, so that increased use of the platform results in an economic advantage, which cannot be quantified on the record (see Article 83(2)(k) of the Regulation), and, in the absence of evidence regarding profits derived from the infringement, this factor is not considered an aggravating circumstance (Guidelines 4/2022, paragraphs 108–110);

− there are no records of corrective measures already imposed on Meta in relation to the same matter, nor of adherence to relevant codes of conduct or certification schemes (Article 83(2)(i) and (j) of the Regulation): neutral factors.

Weighing up the circumstances. In summary, the circumstances set out above, taken as a whole, result in an overall aggravating balance. The mitigating factor referred to in point (c), to which moderate weight is attributed, is in fact outweighed by the aggravating factors referred to in points (d), concerning the degree of liability; (e), concerning the previous infringement; and (f), concerning the lack of cooperation; the other factors are neutral. This results in an increase in the initial amount of 700 million euros – already set at the lower end of the mid-range – which is therefore determined to be 805 million euros. This amount remains fully within the 10–20 per cent range of the ceiling. It is confirmed that the undertaking's financial circumstances are not taken into account further, as they are already reflected in the dynamic ceiling used to determine the initial amount (paragraphs 64 and 66).

Meta requests, as a last resort, that the Authority's response be limited to a non-public reprimand, citing the absence of harm, the limited nature of the data and the de minimis nature of the infringement. The circumstances cited, which have already been considered, do not allow the infringement to be classified as 'minor' within the meaning of recital 148 of the Regulation: the number of users affected, the duration, the structural nature of the infringement and the persistence of part of the conduct necessitate a financial penalty, which, as it must be effective, proportionate and dissuasive (Article 83(1)), must be commensurate with the size of the undertaking, also taking into account the fact that the statutory upper limit does not refer solely to the national scope. Classification as a 'minor' infringement is, moreover, incompatible with the average level of seriousness and the systemic scope established (Guidelines 4/2022, para. 60).

Effectiveness, proportionality and deterrence. The amount thus determined was finally assessed in the light of the requirements of Article 83(1) of the Regulation (Guidelines 4/2022, Chapter 7). From the perspective of effectiveness, the amount is appropriate for penalising the unlawful conduct and for strengthening compliance with the law, also with a view to restoring compliance as required by the corrective measures (para. 135). As regards proportionality, it must be commensurate with both the gravity of the infringement and the size of the undertaking (para. 139): the amount proposed corresponds to approximately 0.47 per cent of global turnover and approximately 1.56 per cent of the group's net profit for the 2025 financial year, and to 11.7 per cent of the statutory ceiling, from which it remains well below; Meta has neither claimed nor documented any inability to pay (paras. 140–141). From the perspective of deterrence, the amount cannot be absorbed as a mere business cost by an undertaking of this size, which ensures specific deterrence; it also signals to market participants that the use of generic operating system permissions to access users' content for different purposes is subject to significant penalties, which ensures general deterrence (paragraphs 142–143). It is therefore not considered appropriate to apply a deterrence multiplier (paragraph 144), nor to reduce the amount.

In view of the above factors, assessed as a whole, and in accordance with the principles of effectiveness, proportionality and deterrence laid down in Article 83, paragraph 1, of the Regulation, it is deemed appropriate to set the amount of the financial penalty imposed on Meta Platforms Ireland Limited at EUR 805,000,000 (eight hundred and five million) for the infringement of Article 122, paragraphs 1 and 2, of the

Code.

6.3. Additional penalty of publication

In conclusion, it is considered that, pursuant to Article 166(7) of the Code and Article 16(1) of the Data Protection Authority's Regulation No 1/2019, the ancillary penalty of publishing this section of the decision containing the injunction order on the, given the particularly reprehensible nature of the conduct: a mechanism providing access to the photo gallery of a very large number of users (approximately 20 million Android users in Italy), set up in 2023 by a global operator via a single authorisation request covering multiple functions, with the Feature preset as active and with insufficient information provided to users to ensure their effective awareness, a situation which is still ongoing for some of them.

FOR THESE REASONS

pursuant to Articles 57 and 83 of the Regulation, the processing of personal data carried out by Meta Platforms Ireland Limited, with its registered office at Merrion Road, Dublin 4, D04 X2K5 (Ireland), registration number IE462932, with address for service for the purposes of these proceedings at the offices of Alessandro Villani and Francesco Amatori, Linklaters Studio Legale Associato (Milan), is hereby declared unlawful for the infringement of Article 122(1) and (2) of the Code, as set out in the grounds;

pursuant to Article 58(2)(d) of the Regulation, Meta Platforms Ireland Limited is hereby required to comply, within sixty days of the date of notification of this decision, with the requirements set out in paragraph 5, first point, of this decision;

Pursuant to Article 58(2)(f) of the Regulation, Meta Platforms Ireland Limited is prohibited, once the time limit referred to in the previous point has elapsed without action, from making the Feature operational for Italian Facebook users on Android devices who have not given their consent in the manner set out in paragraph 5, first point, of this order; Meta Platforms Ireland Limited is also prohibited from processing any information processed via the Feature in the absence of consent obtained in accordance with the specified procedures;

pursuant to Article 58(1)(a) of the Regulation and Article 157 of the Code, Meta Platforms Ireland Limited is ordered to notify the Authority, within thirty days, the steps taken, including for the purposes of resolving the dispute in accordance with Article 166(8) of the Code, as well as, within ninety days of notification of this decision, the steps taken to implement the measures imposed in the preceding points, within the time limits set out in paragraph 5, third point;

IT IS ORDERED

pursuant to Articles 58(2)(i) and 83 of the Regulation, as well as Article 166 of the Code, that Meta Platforms Ireland Limited pay the sum of EUR 805,000,000 (eight hundred and five million) as an administrative fine for the infringement set out in the grounds.

IT IS ORDERED

that the aforementioned company, in the event of failure to settle the dispute in accordance with Article 166(8) of the Code, shall pay the sum indicated above, in accordance with the procedures set out in the annex, within 60 days of service of this order, failing which the consequent enforcement measures shall be taken in accordance with Article 27 of Law No 689/1981.

It is noted that, pursuant to Article 166(8) of the Code, the offender retains the right to settle the dispute by complying with the Data Protection Authority's requirements and by paying – again in accordance with the procedures set out in the annex – an amount equal to half of the penalty imposed within the time limit

specified in Article 10(3) of Legislative Decree of 1 September 2011, No. 150, set for lodging an appeal as indicated below;

IT IS HEREBY ORDERED

▪ pursuant to Article 154-bis(3) of the Code and Article 37 of the Data Protection Authority's Regulation No. 1/2019, that this decision be published on the Data Protection Authority's website;

▪ pursuant to Article 166(7) of the Code and Article 16(1) of the Data Protection Authority's Regulation No. 1/2019, that the injunction order be published on the Data Protection Authority's website;

▪ pursuant to Article 17 of the Data Protection Authority's Regulation No. 1/2019, the recording of the infringements and the measures adopted in accordance with Article 58(2) of the Regulation in the Authority's internal register provided for in Article 57(1)(u) of the Regulation.

Pursuant to Article 78 of the Regulation, as well as Article 152 of the Code and Article 10 of Legislative Decree No. 150 of 1 September 2011, No. 150, an appeal against this decision may be lodged with the ordinary courts by filing an application with the ordinary court of the place specified in the aforementioned Article 10; failure to do so within thirty days of the date of notification of the decision, or within sixty days if the appellant resides abroad, will render the appeal inadmissible.

Rome, 13 November 2026

THE CHAIRMAN
PASQUALE STANZIONE

THE RAPPORTEUR
PASQUALE STANZIONE

THE SECRETARY-GENERAL
LUIGI MONTUORI