Linee Guida

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

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Cronologia delle versioni

Versione 1.0	14 novembre 2023	Adozione degli orientamenti per consultazione pubblica
Versione 2.0	7 ottobre 2024	Adozione degli orientamenti dopo la consultazione pubblica

Sintesi

Nei presenti orientamenti, l'EDPB affronta l'applicabilità dell'articolo 5, paragrafo 3, della direttiva e-privacy a soluzioni tecniche diverse. I presenti orientamenti integrano il parere 9/2014 del Gruppo dell'articolo 29 per la tutela dei dati sull'applicazione della direttiva e-privacy ai dispositivi per il rilevamento delle impronte digitali e mirano a fornire una chiara comprensione delle operazioni tecniche di cui all'articolo 5, paragrafo 3, della direttiva e-privacy.

L'emergere di nuovi metodi di tracciamento che sostituiscono gli strumenti di tracciamento esistenti (ad esempio i cookie, a causa dell'interruzione del supporto per i cookie di terze parti da parte di alcuni fornitori di browser) e creano nuovi modelli di business è diventato un problema critico per la protezione dei dati. Sebbene l'applicabilità dell'articolo 5, paragrafo 3, della direttiva relativa alla vita privata e alle comunicazioni elettroniche sia ben consolidata e attuata per alcune tecnologie di tracciamento come i cookie, è necessario affrontare le ambiguità relative all'applicazione della suddetta disposizione agli strumenti di tracciamento emergenti.

Gli orientamenti individuano tre elementi chiave per l'applicabilità dell'articolo 5, paragrafo 3, della direttiva e-privacy (sezione 2.1), vale a dire «informazioni», «apparecchiature terminali di un abbonato o di un utente», «accesso e archiviazione di informazioni e informazioni conservate». Gli orientamenti forniscono inoltre un'analisi dettagliata di ciascun elemento (sezioni 2.2-2.6).

Nella sezione 3, tale analisi è applicata a un elenco non esaustivo di casi d'uso che rappresentano tecniche comuni, vale a dire:

- tracciamento di URL e pixel;
- elaborazione locale;
- tracciamento basato unicamente sull'indirizzo IP;
- segnalazione intermittente e mediata dell'internet delle cose (IoT);
- identificatore univoco.

Indice

Il Comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettera e), del regolamento 2016/679/UE 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 (in appresso: il «RGPD»),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37 dello stesso, modificati dalla decisione del Comitato misto SEE n. 154/2018, del 6 luglio 2018 ([1]),

visto l'articolo 15, paragrafo 3, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, modificata dalla direttiva 2009/136/CE (in appresso «direttiva e-privacy» o «ePD»),

visto l'articolo 12 e l'articolo 22 del regolamento interno,

HA ADOTTATO I SEGUENTI ORIENTAMENTI:

1 INTRODUZIONE

1. Ai sensi dell'articolo 5, paragrafo 3, della direttiva e-privacy, *«l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente»* è consentita unicamente sulla base del consenso o della necessità per finalità specifiche stabilite in tale articolo. Come rammentato al considerando 24 della direttiva e-privacy ([2]), l'obiettivo di tale disposizione è proteggere le apparecchiature terminali degli utenti, in quanto fanno parte della sfera privata degli utenti. Dalla formulazione dell'articolo risulta che l'articolo 5, paragrafo 3, della direttiva e-privacy non si applica esclusivamente ai cookie, ma anche alle «tecnologie simili». Tuttavia, attualmente non esiste un elenco completo delle operazioni tecniche coperte dall'articolo 5, paragrafo 3, della direttiva e-privacy.

2. Il parere 9/2014 del Gruppo dell'articolo 29 per la tutela dei dati (in appresso: «WP29») sull'applicazione della direttiva e-privacy ai dispositivi per la raccolta delle impronte digitali (in appresso: «parere 9/2014 del WP29») ha già chiarito che la raccolta delle impronte digitali rientra nell'ambito di applicazione tecnico dell'articolo 5, paragrafo 3, della direttiva e-privacy ([3]), ma a causa dei nuovi progressi tecnologici nel settore delle tecnologie sono necessari ulteriori orientamenti per quanto riguarda le tecniche di tracciamento attualmente osservate. Il panorama tecnico si è sviluppato nel corso dell'ultimo decennio, con l'uso crescente di identificatori integrati nei sistemi operativi,

([1]) Nel presente documento, con «Stati membri» ci si riferisce agli «Stati membri del SEE».
([2]) «Le apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno parte della sfera privata dell'utente, che deve essere tutelata ai sensi della convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali. I cosiddetti spyware, bug web, identificatori nascosti e altri dispositivi simili possono entrare nel terminale degli utenti a loro insaputa per ottenere l'accesso alle informazioni, memorizzare informazioni nascoste o tracciare le attività dell'utente e possono interferire gravemente con la vita privata di tali utenti. L'uso di tali dispositivi dovrebbe essere consentito solo per scopi legittimi, con la conoscenza degli utenti interessati».
([3]) Parere 9/2014 del WP29, pag. 11.

nonché la creazione di nuovi strumenti che consentano la memorizzazione di informazioni nelle apparecchiature terminali.

3. Le ambiguità relative all'ambito di applicazione dell'articolo 5, paragrafo 3, della direttiva e-privacy hanno creato incentivi per l'attuazione di soluzioni alternative per il tracciamento degli utenti di internet e hanno portato alla tendenza ad aggirare gli obblighi giuridici previsti dall'articolo 5, paragrafo 3, della direttiva e-privacy. Tutte queste situazioni sollevano preoccupazioni e richiedono un'analisi supplementare al fine di integrare i precedenti orientamenti forniti dal comitato europeo per la protezione dei dati.

4. La finalità dei presenti orientamenti è di condurre un'analisi tecnica dell'ambito di applicazione dell'articolo 5, paragrafo 3, della direttiva e-privacy, ossia chiarire ciò che è tecnicamente coperto dalla frase «*per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente*». I presenti orientamenti non affrontano le circostanze in cui un'operazione di trattamento può rientrare nelle esenzioni dall'obbligo di consenso previste dalla direttiva e-privacy ([4]), in quanto tali circostanze dovrebbero essere analizzate caso per caso tenendo conto del(i) recepimento(i) dello Stato membro o dei pertinenti Stati membri e degli orientamenti emanati dalle autorità nazionali competenti.

5. Un elenco non esaustivo di casi d'uso specifici sarà analizzato nella parte finale dei presenti orientamenti.

2 ANALISI

2.1 Elementi chiave per l'applicabilità dell'articolo 5, paragrafo 3, della direttiva e-privacy

6. L'articolo 5, paragrafo 3, della direttiva e-privacy si applica se:

   a. **CRITERIO A:** le operazioni effettuate riguardano le «*informazioni*». Va notato che il termine utilizzato non è «dati personali», ma «informazioni».

   b. **CRITERIO B:** le operazioni effettuate coinvolgono un'«*apparecchiatura terminale*» di un abbonato o di un utente (B.1), il che comporta la necessità di valutare la nozione *di una «rete pubblica di comunicazione»* (B.2).

   c. **CRITERIO C:** le operazioni effettuate costituiscono effettivamente una «*memorizzazione*» (C.1) o un «*accesso*» (C.2). Queste due nozioni possono essere studiate indipendentemente, come ricordato nel parere 9/2014 del WP29: *«L'uso delle parole "sottoposte ad archiviazione o ad accesso" indica che non è necessario che l'archiviazione e l'accesso avvengano nell'ambito della stessa comunicazione o che siano effettuate dallo stesso soggetto» ([5]).*

Per ragioni di leggibilità, l'entità che ottiene l'accesso alle informazioni archiviate nell'apparecchiatura terminale dell'utente sarà di seguito indicata come «entità che accede».

([4]) Come indicato nell'articolo 5, paragrafo 3, della direttiva e-privacy: «*Ciò non vieta l'eventuale archiviazione tecnica o l'accesso al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio.*»
([5]) Parere 9/2014 del WP29, pag. 8.

2.2 Nozione di «informazione» – Criterio A

7. Come espresso nel CRITERIO A, questa sezione specifica ciò che rientra nella nozione di «informazione». La scelta del termine «informazione», che comprende una categoria più ampia rispetto alla semplice nozione di dati personali, è legata all'ambito di applicazione della direttiva e-privacy.

8. L'obiettivo dell'articolo 5, paragrafo 3, della direttiva consiste nel proteggere la sfera privata degli utenti, come indicato nel suo considerando 24: «*Le apparecchiature terminali degli utenti delle reti di comunicazione elettronica e tutte le informazioni conservate su tali apparecchiature fanno parte della sfera privata degli utenti che necessitano di protezione ai sensi della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*».

9. In realtà, gli scenari che si intromettono in questa sfera privata anche senza coinvolgere alcun dato personale sono esplicitamente coperti dalla formulazione dell'articolo 5, paragrafo 3, e del considerando 24 della direttiva e-privacy, ad esempio la memorizzazione di virus nell'apparecchiatura terminale dell'utente. Ciò dimostra che la definizione del termine «informazione» non dovrebbe essere limitata alla proprietà di essere correlata a una persona fisica identificata o identificabile.

10. Ciò è stato confermato dalla Corte di giustizia dell'UE: «*Detta tutela si applica a qualsiasi informazione archiviata in tale apparecchiatura terminale, indipendentemente dal fatto che si tratti o meno di dati personali ed è volta, in particolare, come risulta dal medesimo considerando, a tutelare gli utenti dal rischio che identificatori occulti o altri dispositivi analoghi si introducano nell'apparecchiatura terminale dell'utente a sua insaputa.*» ([6])

11. La questione se l'origine di tali informazioni e i motivi per cui sono conservate nell'apparecchiatura terminale debba essere presa in considerazione al momento di valutare l'applicabilità dell'articolo 5, paragrafo 3, della direttiva e-privacy è stata precedentemente chiarita. Ad esempio, nel parere 9/2014 del WP29: «*Non è corretto interpretare ciò nel senso che il terzo non necessiti del consenso per accedere a tali informazioni semplicemente perché non le ha archiviate. L'obbligo del consenso si applica anche quando si accede a un valore di sola lettura (ad esempio, richiedendo l'indirizzo MAC di un'interfaccia di rete attraverso l'API del sistema operativo).*» ([7]).

12. In conclusione, la nozione di informazioni annovera sia i dati non personali sia i dati personali, indipendentemente dal modo in cui tali dati sono stati conservati e da chi, vale a dire se da un soggetto esterno (comprese anche le entità diverse da quella a cui ha accesso), dall'utente, da un fabbricante o da qualsiasi altro scenario.

2.3 Nozione di «apparecchiature terminali di un sottoscrittore o di un utente» — criterio B.1

13. La presente sezione si basa sulla definizione utilizzata nella direttiva 2008/63/CE e cui fa riferimento l'articolo 2 della direttiva (UE) 2018/1972, in cui le «apparecchiature terminali» sono definite come segue: «*le apparecchiature allacciate direttamente o indirettamente all'interfaccia di una rete pubblica di telecomunicazioni per trasmettere, trattare o ricevere informazioni; in entrambi i casi di allacciamento, diretto o indiretto, esso può essere realizzato via cavo, fibra ottica o via*

([6]) Sentenza della Corte di giustizia del 1º ottobre 2019, Planet 49, causa C-673/17, ECLI:EU:C:2019:801, punto 70.
([7]) Parere 9/2014 del WP29, pag. 8.

elettromagnetica; un allacciamento è indiretto se l'apparecchiatura è interposta fra il terminale e l'interfaccia della rete pubblica» ([8]).

14. Il considerando 24 della direttiva e-privacy fornisce una chiara comprensione del ruolo dell'apparecchiatura terminale per la protezione offerta dall'articolo 5, paragrafo 3, della stessa direttiva. La ePD protegge la privacy degli utenti non solo in relazione alla riservatezza delle loro informazioni, ma anche salvaguardando l'integrità dell'apparecchiatura terminale dell'utente. Questa comprensione guiderà l'interpretazione del concetto di apparecchiatura terminale in tutti i presenti orientamenti.

15. L'articolo 3 della direttiva e-privacy stabilisce che, ai fini dell'applicazione della direttiva, il trattamento dei dati personali deve essere effettuato in relazione alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche. Ciò implica che un dispositivo debba essere utilizzabile in connessione con tale servizio e che, per essere qualificato come apparecchiatura terminale, debba essere collegato o collegabile ([9]) all'interfaccia di una rete pubblica di comunicazione. L'EDPB osserva che le modifiche apportate nel 2009 ([10]) nel testo dell'articolo 5, paragrafo 3, della direttiva e-privacy hanno esteso la protezione delle apparecchiature terminali, cancellando il riferimento all'«uso della rete di comunicazione elettronica» come mezzo per memorizzare informazioni o per ottenere accesso alle informazioni archiviate nell'apparecchiatura terminale. Pertanto, fintanto che un dispositivo dispone di un'interfaccia di rete che lo rende idoneo alla connessione (anche se tale connessione non è in atto), l'articolo 5, paragrafo 3, della direttiva si applica a tutti i soggetti che memorizzano e accedono alle informazioni già memorizzate nell'apparecchiatura terminale, a prescindere dal mezzo di accesso all'apparecchiatura terminale e dal fatto che sia collegata o scollegata da una rete.

16. Le apparecchiature che fanno parte della rete pubblica di comunicazione elettronica non sarebbero considerate apparecchiature terminali ai sensi dell'articolo 5, paragrafo 3, della direttiva e-privacy ([11]).

17. Un'apparecchiatura terminale può essere composta da un numero qualsiasi di singoli pezzi di hardware, che insieme la formano. Questo può assumere o meno la forma di un dispositivo fisicamente chiuso che ospita tutto il display, l'elaborazione, l'archiviazione e l'hardware periferico (ad esempio, smartphone, laptop, dispositivi di archiviazione collegati alla rete, automobili o TV connesse, occhiali intelligenti).

18. La direttiva riconosce che la protezione della riservatezza delle informazioni memorizzate sull'apparecchiatura terminale dell'utente e l'integrità dell'apparecchiatura terminale dell'utente non si limita alla protezione della sfera privata delle persone fisiche, ma riguarda anche il diritto al rispetto

([8]) Direttiva 2008/63/CE della Commissione, del 20 giugno 2008, relativa alla concorrenza sui mercati delle apparecchiature terminali di telecomunicazioni (versione codificata), articolo 1, paragrafo 1.

([9]) Ovvero, avere le capacità tecniche per essere connessi alla rete anche se tale connessione non è attualmente presente.

([10]) Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori (Testo rilevante ai fini del SEE), GU L 337 del 18.12.2009, articolo 2, paragrafo 5 e considerando 65.

([11]) Per individuare i limiti della rete in contesti diversi, fare riferimento agli orientamenti del BEREC sugli approcci comuni all'identificazione del punto di terminazione della rete in diverse topologie della rete [BoR (20) 46].

della loro corrispondenza o gli interessi legittimi delle persone giuridiche ([12]). Pertanto, un'apparecchiatura terminale che consenta di attuare questa corrispondenza e gli interessi legittimi delle persone giuridiche è protetta ai sensi dell'articolo 5, paragrafo 3, della direttiva e-privacy.

19. L'utente o l'abbonato può possedere, affittare o ricevere in altro modo l'apparecchiatura terminale. Più utenti o abbonati possono condividere la stessa apparecchiatura terminale.

20. Questa protezione è garantita dalla direttiva e-privacy all'apparecchiatura terminale associata all'utente o all'abbonato e non dipende dal fatto che l'utente abbia predisposto il mezzo di accesso (ad esempio se ha avviato la comunicazione elettronica) o anche dal fatto che l'utente sia a conoscenza di tale mezzo di accesso.

2.4 Nozione di «rete pubblica di comunicazione» – Criterio B.2

21. Poiché la situazione disciplinata dalla direttiva e-privacy è quella relativa «*alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nella Comunità.*» ([13]) e la definizione di apparecchiatura terminale menziona specificamente la nozione di «*rete pubblica di comunicazione*», è fondamentale chiarire tale nozione per individuare il contesto in cui si applica l'articolo 5, paragrafo 3, della predetta direttiva.

22. La nozione di rete di comunicazione elettronica non è definita nel quadro della direttiva stessa. Tale concetto è stato originariamente menzionato nella direttiva 2002/21/CE (la direttiva quadro) che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica ([14]), successivamente sostituita dall'articolo 2, paragrafo 1, della direttiva 2018/1972 (il codice europeo delle comunicazioni elettroniche). Adesso recita come segue:

> *«reti di comunicazione elettronica»: i sistemi di trasmissione, basati o meno su un'infrastruttura permanente o una capacità di amministrazione centralizzata, e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa internet), i sistemi per il trasporto via cavo della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti utilizzate per la diffusione radiotelevisiva, e le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato. ([15])*

23. Questa definizione è neutra rispetto alle tecnologie di trasmissione. Una rete di comunicazione elettronica, secondo questa definizione, è qualsiasi sistema di rete che consente la trasmissione di segnali elettronici tra i suoi nodi, indipendentemente dalle apparecchiature e dai protocolli utilizzati.

24. La nozione di rete di comunicazione elettronica ai sensi della direttiva 2018/1972 non dipende dalla natura pubblica o privata dell'infrastruttura, né dal modo in cui la rete è installata o gestita [«*basata o*

([12]) Come in effetti rammentato all'articolo 2, paragrafo 13, della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche, l'utente può essere una persona fisica o giuridica.
([13]) Articolo 3 della direttiva e-privacy.
([14]) Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro)
([15]) Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche (rifusione), testo rilevante ai fini del SEE, articolo 2, paragrafo 1.

meno su un'infrastruttura permanente o sulla capacità di amministrazione centralizzata» ([16])]. Di conseguenza, la definizione di rete di comunicazione elettronica, ai sensi dell'articolo 2 della direttiva 2018/1972, è abbastanza ampia da coprire qualsiasi tipo di infrastruttura. Sono comprese le reti gestite o meno da un operatore, le reti cogestite da un gruppo di operatori o anche le reti ad hoc nelle quali un'apparecchiatura terminale può unirsi dinamicamente o lasciare una rete di altre apparecchiature terminali utilizzando protocolli di trasmissione a corto raggio.

25. Questa definizione di rete non prevede alcuna limitazione per quanto riguarda il numero di apparecchiature terminali presenti nella rete in qualsiasi momento. Alcuni programmi di collegamento in rete si basano su nodi che trasmettono le informazioni in maniera mirata a nodi attualmente connessi ([17]) e possono avere, in un certo momento, fino a due colleghi in comunicazione. Tali casi rientrerebbero nell'ambito di applicazione generale della direttiva e-privacy, nella misura in cui il protocollo di rete consente l'ulteriore inclusione dei pari.

26. La disponibilità al pubblico della rete di comunicazione è necessaria affinché il dispositivo sia considerato un'apparecchiatura terminale e, di conseguenza, ai fini dell'applicabilità dell'articolo 5, paragrafo 3, della direttiva e-privacy. Va notato che il fatto che la rete sia messa a disposizione di un sottoinsieme limitato del pubblico (ad esempio, gli abbonati, paganti o meno, soggetti a condizioni di ammissibilità) non rende tale rete privata ([18]).

2.5 Nozione di «ottenimento dell'accesso» – Criterio C.1

27. Per inquadrare correttamente la nozione di «ottenimento dell'accesso», è importante considerare l'ambito di applicazione della direttiva e-privacy, indicato nel suo articolo 1: «*assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità*».

28. In poche parole, la direttiva ePD è uno strumento giuridico che tutela la privacy e che mira a proteggere la riservatezza delle comunicazioni e l'integrità dei dispositivi. Nel considerando 24 della direttiva e-privacy si chiarisce che, nel caso delle persone fisiche, l'apparecchiatura terminale dell'utente fa parte della sua sfera privata e che l'accesso alle informazioni memorizzate su di essa a sua insaputa può costituire una grave intrusione nella sua privacy.

29. Anche le persone giuridiche sono tutelate dalla direttiva e-privacy ([19]). Di conseguenza, la nozione di «accesso» di cui all'articolo 5, paragrafo 3, della direttiva e-privacy deve essere interpretata in modo da salvaguardare tali diritti dalla violazione da parte di terzi.

30. La memorizzazione delle informazioni o l'ottenimento dell'accesso possono essere operazioni indipendenti ed eseguite da entità indipendenti. L'archiviazione delle informazioni e l'accesso alle informazioni già archiviate non devono necessariamente essere entrambi presenti ai fini dell'applicazione dell'articolo 5, paragrafo 3, della direttiva e-privacy.

([16]) Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche (rifusione), testo rilevante ai fini del SEE, articolo 2, paragrafo 1.
([17]) Ad esempio, nel contesto di uno schema di creazione di reti con tolleranza al ritardo che attua «tecniche di archiviazione e sviluppo» come il progetto Briar open source.
([18]) Per un'ulteriore analisi sull'identificazione delle reti pubbliche di comunicazione, si rimanda agli orientamenti del BEREC sull'attuazione del regolamento sull'apertura di internet [BoR (20) 112].
([19]) Considerando 26 della direttiva e-privacy; cfr. il precedente punto 17.

31. Come specificato nel parere 9/2014 del WP29: «*L'uso delle parole "sottoposte ad archiviazione o ad accesso" indica che non è necessario che l'archiviazione e l'accesso avvengano nell'ambito della stessa comunicazione o che siano effettuate dallo stesso soggetto. Le informazioni che vengono archiviate da un soggetto (comprese le informazioni archiviate dall'utente o dal fabbricante del dispositivo) alle quali successivamente accede un altro soggetto rientrano quindi nel campo d'applicazione dell'articolo 5, paragrafo 3* ([20])» Di conseguenza, non vi sono restrizioni all'origine delle informazioni sulle apparecchiature terminali ai fini dell'applicazione della nozione di accesso.

32. Ogniqualvolta un'entità adotta misure per ottenere l'accesso alle informazioni archiviate nell'apparecchiatura terminale, si applica l'articolo 5, paragrafo 3, della direttiva e-privacy. Di solito questo comporta che l'entità di accesso invii proattivamente istruzioni specifiche all'apparecchiatura terminale per ricevere indietro le informazioni desiderate. È il caso, ad esempio, dei cookie, in cui l'entità che accede istruisce l'apparecchiatura terminale a inviare proattivamente informazioni a ogni successiva chiamata al protocollo di trasferimento ipertestuale («HTTP»).

33. Questo vale anche quando l'entità che accede distribuisce un software sull'apparecchiatura terminale dell'utente che viene memorizzato e che poi chiamerà in modo proattivo un endpoint dell'interfaccia di programmazione dell'applicazione («API») attraverso la rete. Ulteriori esempi includerebbero il codice JavaScript, in cui l'entità che accede istruisce il browser dell'utente di inviare richieste asincrone con le informazioni mirate. Tale accesso rientra chiaramente nell'ambito di applicazione dell'articolo 5, paragrafo 3, della direttiva e-privacy, in quanto il soggetto che ha effettuato l'accesso incarica esplicitamente l'apparecchiatura terminale di inviare le informazioni.

34. In alcuni casi, l'entità che ordina all'apparecchiatura terminale di rinviare i dati mirati e l'entità che riceve le informazioni potrebbero non essere le stesse. Ciò può derivare dalla messa a disposizione e/o dall'uso di un meccanismo comune tra le due entità. Ordinare al dispositivo di inviare informazioni già memorizzate [ad esempio mediante l'uso di un protocollo o di un SDK ([21]) che implica l'invio proattivo di informazioni da parte dell'apparecchiatura terminale] rende possibile un'intrusione nell'apparecchiatura terminale, pertanto tale accesso determina l'applicabilità dell'articolo 5, paragrafo 3, della direttiva. Come osservato nel parere 09/2014 del WP29, ciò può verificarsi quando un sito web istruisce l'apparecchiatura terminale a inviare informazioni a servizi pubblicitari di terzi attraverso l'inserimento di un pixel di tracciamento ([22]). Questo caso d'uso viene ulteriormente sviluppato nella sezione 3.1.

2.6 Concetti di memorizzazione delle informazioni» e «informazioni archiviate» – Criterio C.2

35. L'archiviazione delle informazioni ai sensi dell'articolo 5, paragrafo 3, della direttiva e-privacy si riferisce all'inserimento di informazioni su un supporto fisico di archiviazione elettronica che fa parte dell'apparecchiatura terminale dell'utente o dell'abbonato ([23]).

36. In genere, le informazioni non vengono memorizzate nell'apparecchiatura terminale di un utente o di un abbonato attraverso l'accesso diretto alla memoria del dispositivo da parte di un altro soggetto, ma piuttosto istruendo il software dell'apparecchiatura terminale a generare informazioni specifiche. La memorizzazione effettuata mediante tali istruzioni è considerata avviata direttamente dall'altra parte.

([20]) Parere 9/2014 del WP29, pag. 8.
([21]) Un SDK («kit di sviluppo software») è un insieme di strumenti di sviluppo software messi a disposizione per facilitare la creazione di software applicativi.
([22]) Parere 9/2014 del WP29, pag. 9.
([23]) Secondo la definizione di cui alla sezione 2.3 dei presenti orientamenti.

Ciò include l'uso di protocolli consolidati, come la memorizzazione dei cookie del browser, e di software personalizzati, indipendentemente da chi ha creato o installato i protocolli o il software sull'apparecchiatura terminale.

37. La direttiva e-privacy non pone alcun limite superiore o inferiore in merito alla durata della persistenza delle informazioni su un supporto di memorizzazione da considerare memorizzato, né vi è un limite superiore o inferiore per quanto riguarda la quantità di informazioni da conservare.

38. Analogamente, la nozione di archiviazione non dipende dal tipo di supporto su cui le informazioni sono archiviate. Tra gli esempi tipici rientrano i dischi rigidi («HDD»), i dischi a stato solido («SSD»), la memoria di sola lettura programmabile e cancellabile elettricamente («EEPROM») e la memoria a accesso casuale («RAM»), ma gli scenari meno tipici che coinvolgono un supporto come la memoria a nastro magnetico o la memoria centrale di elaborazione («CPU») non sono esclusi dall'ambito di applicazione. Il supporto di memorizzazione può essere collegato internamente (ad esempio attraverso una connessione SATA) ed esternamente (ad esempio attraverso una connessione USB)

39. Per «informazioni memorizzate» si intendono le informazioni già presenti nell'apparecchiatura terminale, indipendentemente dalla fonte o dalla natura di tali informazioni. Ciò comprende qualsiasi risultato derivante dall'archiviazione delle informazioni ai sensi dell'articolo 5, paragrafo 3, della direttiva sulle pratiche commerciali elettroniche, come descritto in precedenza (da parte della stessa parte che otterrebbe successivamente l'accesso o da parte di un altro terzo). Comprende inoltre i risultati dei processi di archiviazione delle informazioni al di là dell'ambito di applicazione dell'articolo 5, paragrafo 3, della direttiva e-privacy, quali: la memorizzazione sull'apparecchiatura terminale da parte dell'utente o dell'abbonato stesso o da parte di un fabbricante di hardware (come gli indirizzi MAC dei controllori dell'interfaccia di rete), sensori integrati nell'apparecchiatura terminale o processi e programmi eseguiti sull'apparecchiatura terminale, che possono o meno produrre informazioni che dipendono o derivano da informazioni memorizzate.

3 CASI DI UTILIZZO

40. Come evidenziato nell'introduzione dei presenti orientamenti ([24]), essi non analizzano l'applicazione delle esenzioni all'obbligo di ottenere il consenso di cui all'articolo 5, paragrafo 3, della direttiva e-privacy. L'EDPB ricorda che, per tutti i casi in cui vi sia una memorizzazione di informazioni o l'ottenimento dell'accesso a informazioni già archiviate, dovrebbe essere valutato se sia necessario un consenso o se si possa applicare un'esenzione ai sensi dell'articolo 5, paragrafo 3, della direttiva e-privacy. Il lettore dovrebbe pertanto prendere in considerazione le esenzioni nel loro caso d'uso, unitamente a questa analisi tecnica.

41. Fermo restando il contesto specifico in cui possono essere utilizzate le categorie tecniche necessarie per qualificare l'applicabilità dell'articolo 5, paragrafo 3, della direttiva e-privacy, è possibile individuare, in modo non esaustivo, ampie categorie di identificatori e informazioni che sono ampiamente utilizzate e possono essere soggette all'applicabilità dell'articolo 5, paragrafo 3, della direttiva e-privacy.

42. La comunicazione in rete si basa di solito su un modello a più livelli che richiede l'uso di identificatori per consentire una corretta istituzione ed esecuzione della comunicazione. La comunicazione di tali identificatori agli attori remoti è istruita mediante software sulla base di protocolli di comunicazione concordati. Come indicato in precedenza, il fatto che l'ente ricevente possa non essere l'ente che

([24]) Cfr. il punto 4 sopra.

ordina l'invio di informazioni non preclude l'applicazione dell'articolo 5, paragrafo 3, della direttiva. Ciò potrebbe riguardare gli identificatori di instradamento, quali l'indirizzo MAC o IP dell'apparecchiatura terminale, ma anche gli identificatori di sessione (SSRC, identificatore Websocket) o i token di autenticazione.

43. Allo stesso modo, il protocollo applicativo può includere diversi meccanismi per fornire dati di contesto (come l'intestazione HTTP che include il campo «accept» o l'agente utente), un meccanismo di caching [come ETag ([25])] o altre funzionalità [tra cui i cookie o HSTS ([26])]. Ancora una volta, il ricorso a tali meccanismi per la raccolta di informazioni (ad esempio nel contesto del rilevamento delle impronte digitali ([27]) o del tracciamento degli identificatori di risorse) può portare all'applicazione dell'articolo 5, paragrafo 3, della direttiva e-privacy.

44. D'altro canto, vi sono alcuni contesti in cui le applicazioni locali installate nell'apparecchiatura terminale utilizzano alcune informazioni strettamente all'interno del terminale, come potrebbe accadere per le API del sistema per smartphone (accesso a fotocamera, microfono, sensore GPS, chip acceleratore, chip radio, accesso ai file locali, elenco di contatti, accesso agli identificatori, ecc.). Questo potrebbe anche essere il caso dei browser web che elaborano le informazioni memorizzate o generate all'interno del dispositivo (quali cookie, archiviazione locale, WebSQL o anche le informazioni fornite dagli utenti stessi). L'utilizzo di tali informazioni da parte di un'applicazione non costituirebbe un «accesso a informazioni già archiviate» ai sensi dell'articolo 5, paragrafo 3, della direttiva e-privacy, 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.

45. Infine, in alcuni casi degli operatori distribuiscono elementi software dolosi, ad esempio software di estrazione di criptografia o, più in generale, software maligni, sfruttando le capacità di elaborazione dell'apparecchiatura terminale a vantaggio dell'operatore distributore. La distribuzione di detti software maligni nelle apparecchiature terminali dell'utente costituirebbe un'«archiviazione» ai sensi dell'articolo 5, paragrafo 3, della direttiva e-privacy. Inoltre, se il software dovesse stabilire una connessione di rete per inviare informazioni in una fase successiva, ciò costituirebbe un «accesso» ai sensi dell'articolo 5, paragrafo 3, della direttiva e-privacy.

46. Per un sottoinsieme di queste categorie che presentano un interesse specifico, a causa del loro uso diffuso o perché è giustificato uno studio specifico in relazione alle circostanze del loro uso, si fornisce di seguito un'analisi specifica.

3.1 Tracciamento di URL e pixel

47. Un pixel di tracciamento è un collegamento ipertestuale a una risorsa, di solito un file di immagine, integrato in un contenuto come un sito web o un messaggio di posta elettronica. Questo pixel di solito non persegue alcun obiettivo connesso al contenuto richiesto stesso; il suo unico scopo è quello di stabilire automaticamente una comunicazione da parte del cliente al paese ospitante del pixel, che altrimenti non si sarebbe verificata. Tuttavia, questo non è sistematico e i pixel di tracciamento possono essere creati anche aggiungendo informazioni supplementari alle immagini di caricamento dei collegamenti ipertestuali che sono rilevanti per il contenuto visualizzato dall'utente. Istituzione

([25]) Per HTTP ETag si intende un identificatore che consente di effettuare richieste condizionali basate sulla validità dei dati client memorizzati nella cache.
([26]) HTTP Strict Transport Security (HSTS) consente ai server di specificare quali risorse dovrebbero sempre essere richieste utilizzando connessioni HTTPS.
([27]) Come osservato nell'introduzione, si veda il parere 9/2014 del Gruppo dell'articolo 29 per la tutela dei dati sull'applicazione della direttiva e-privacy ai dispositivi per la raccolta delle impronte digitali.

della comunicazione trasmette varie informazioni all'ospite del pixel, a seconda del caso d'uso specifico.

48. Nel caso di un messaggio di posta elettronica, il mittente può includere un pixel di tracciamento per rilevare quando il destinatario legge il messaggio. I pixel di tracciamento sui siti web possono essere collegati a un'entità che raccoglie molte di queste richieste ed è quindi in grado di tracciare il comportamento degli utenti. Tali pixel di tracciamento possono anche contenere identificatori, metadati o contenuti aggiuntivi come parte del link. Tali punti di dati possono essere aggiunti dal titolare del sito web, eventualmente in relazione all'attività dell'utente su tale sito web, in modo da generare relazioni d'uso analitiche. Possono anche essere generati dinamicamente attraverso la logica applicativa lato client fornita dall'entità.

49. I link di tracciamento possono funzionare allo stesso modo, ma l'identificatore viene aggiunto all'indirizzo del sito web. Quando l'utente visita il localizzatore uniforme di risorse («URL»), il sito web mirato carica la risorsa richiesta ma raccoglie anche un identificatore che non è pertinente in termini di identificazione della risorsa. Sono molto comunemente utilizzati dai siti web di commercio elettronico per identificare l'origine della loro fonte di traffico in entrata. Ad esempio, tali siti web possono fornire collegamenti monitorati ai partner da utilizzare sul loro dominio, in modo che il sito web di commercio elettronico sappia quale dei loro partner è responsabile di una vendita e paghi una commissione, una pratica nota come marketing affiliato.

50. Sia i link di tracciamento che i pixel di tracciamento possono essere distribuiti attraverso un'ampia varietà di canali, ad esempio tramite posta elettronica, siti web o anche, nel caso dei link di tracciamento, attraverso qualsiasi tipo di sistema di messaggistica di testo. Tale distribuzione all'apparecchiatura terminale dell'utente costituisce effettivamente una memorizzazione, quantomeno attraverso il meccanismo di caching del software lato cliente. In quanto tale, l'articolo 5, paragrafo 3, della direttiva e-privacy è applicabile anche se la memorizzazione non è permanente.

51. L'aggiunta di informazioni di tracciamento agli URL o alle immagini (pixel) inviate all'utente costituisce un'istruzione per l'apparecchiatura terminale di rinviare le informazioni mirate (l'identificatore specificato). Nel caso di pixel di tracciamento costruiti dinamicamente, è la distribuzione della logica applicativa (di solito un codice JavaScript) a costituire l'istruzione. Di conseguenza, si può ritenere che la raccolta di identificatori fornita attraverso tali meccanismi di tracciamento costituisca un «accesso» ai sensi dell'articolo 5, paragrafo 3, della direttiva e-privacy, pertanto si applica anche a tale fase.

3.2 Elaborazione locale

52. Alcune tecnologie si basano su processi locali ordinati da software distribuiti sulle apparecchiature terminali degli utenti, in cui le informazioni prodotte dal trattamento locale sono poi messe a disposizione di soggetti selezionati attraverso API sul lato del cliente. Questo può essere il caso, ad esempio, di un'API fornita dal browser web, in cui i risultati generati localmente possono essere consultati a distanza.

53. Se in qualsiasi momento, ad esempio nel codice lato cliente, le informazioni trattate sono messe a disposizione di un terzo, ad esempio restituite sulla rete a un server, tale operazione (su istruzione dell'entità che produce il codice lato cliente distribuito sull'apparecchiatura terminale utente) costituirebbe un «accesso a informazioni già archiviate». Il fatto che tali informazioni siano prodotte a livello locale non preclude l'applicazione dell'articolo 5, paragrafo 3, della direttiva e-privacy.

3.3 Tracciamento basato unicamente sull'indirizzo IP

54. Alcuni fornitori stanno sviluppando soluzioni che si basano solo sulla raccolta di una componente, vale a dire l'indirizzo IP, al fine di tracciare la navigazione ([28]) dell'utente, in alcuni casi su più domini. In tale contesto, l'articolo 5, paragrafo 3, della direttiva potrebbe applicarsi anche se l'istruzione di mettere a disposizione l'indirizzo IP è stata impartita da un'entità diversa da quella ricevente.

55. L'ottenimento dell'accesso agli indirizzi IP comporterebbe tuttavia l'applicazione dell'articolo 5, paragrafo 3, della direttiva e-privacy solo nei casi in cui tali informazioni provengano dall'apparecchiatura terminale di un abbonato o di un utente. Sebbene non si verifichi sistematicamente [ad esempio quando viene attivata la CGNAT ([29])], l'IPv4 statico in uscita proveniente dal router di un utente rientrerebbe in tale caso, così come gli indirizzi IPV6 poiché sono in parte definiti dal paese ospitante. A meno che l'entità non sia in grado di garantire che l'indirizzo IP non provenga dalle apparecchiature terminali di un utente o di un abbonato, essa deve adottare tutte le misure a norma dell'articolo 5, paragrafo 3, della direttiva e-privacy.

56. Sebbene i presenti orientamenti non analizzino l'applicazione delle esenzioni all'obbligo di raccogliere il consenso di cui all'articolo 5, paragrafo 3, della direttiva e-privacy, è importante ricordare ancora una volta che l'applicabilità di tale articolo non implica sistematicamente che il consenso debba essere raccolto. L'EDPB ricorda pertanto che in ciascun caso dovrebbe essere valutato se sia necessario un consenso o se possa applicarsi una deroga ai sensi dell'articolo 5, paragrafo 3, della direttiva e-privacy ([30]).

3.4 Segnalazione dell'internet delle cose intermittente e mediata

57. I dispositivi IoT (internet delle cose) producono informazioni in modo continuo nel tempo, ad esempio attraverso sensori incorporati nel dispositivo, che possono essere o meno pretrattati localmente. In molti casi, le informazioni vengono rese disponibili a un server remoto, ma le modalità di raccolta possono variare.

58. Alcuni dispositivi IoT hanno una connessione diretta a una rete di comunicazione pubblica con una scheda SIM cellulare. Altri possono avere una connessione indiretta a una rete di comunicazione pubblica, ad esempio attraverso l'uso del WIFI o la trasmissione di informazioni a un altro dispositivo attraverso una connessione punto-punto (ad esempio, tramite Bluetooth). L'altro dispositivo può essere ad esempio uno smartphone o un gateway dedicato che può o meno pre-elaborare le informazioni prima di inviarle al server.

59. I dispositivi IoT potrebbero essere istruiti dal produttore a trasmettere sempre in streaming le informazioni raccolte, pur conservando prima le informazioni nella cache locale, ad esempio fino a quando non è disponibile una connessione.

60. In ogni caso, il dispositivo IoT, se connesso (direttamente o indirettamente) a una rete di comunicazione pubblica, sarebbe esso stesso considerato un'apparecchiatura terminale. Il fatto che le informazioni siano trasmesse in streaming o messe in cache per la segnalazione intermittente non modifica la natura di tali informazioni. In entrambe le situazioni si applicherebbe l'articolo 5,

([28]) Ciò si aggiunge e prescinde dall'uso e dalla funzione di un indirizzo IP per la creazione e l'inoltro o la trasmissione di comunicazioni tecniche sottostanti, o dal fatto che possa o meno trattarsi di dati personali (ai fini dell'analisi e-privacy, si tratta di «informazioni»).
([29]) Il Carrier-grade NAT o CGNAT è utilizzato dai provider di servizi internet per massimizzare l'uso dello spazio limitato degli indirizzi IP. Raggruppa un certo numero di abbonati sotto lo stesso indirizzo IP pubblico.
([30]) Il parere 9/2014 del WP29 fornisce alcuni esempi di casi in cui il consenso potrebbe non essere necessario.

paragrafo 3, della direttiva e-privacy in quanto, attraverso l'istruzione del codice sul dispositivo IoT di inviare i dati memorizzati dinamicamente al server remoto, si verifica un «accesso».

3.5 Identificatore univoco

61. Uno strumento comune utilizzato dalle imprese è il concetto di «identificatori unici» o «identificatori persistenti». Tali identificatori possono essere ricavati da dati personali persistenti (nome e cognome, indirizzo di posta elettronica, numero di telefono ecc.), che sono oggetto di hashing sul dispositivo dell'utente, raccolti e condivisi tra diversi titolari del trattamento per identificare in modo univoco una persona su diversi set di dati [utilizzo dei dati raccolti attraverso l'uso di un sito web o di un'applicazione, gestione delle relazioni con i clienti (CRM) relativi all'acquisto o all'abbonamento online o offline, ecc.]. Sui siti web, i dati personali persistenti sono generalmente ottenuti nel contesto dell'autenticazione o dell'iscrizione alle newsletter.

62. Come indicato in precedenza, il fatto che le informazioni vengano inserite dall'utente non preclude l'applicazione dell'articolo 5, paragrafo 3, della direttiva sulla protezione dei dati per quanto riguarda la memorizzazione, in quanto tali informazioni vengono memorizzate temporaneamente sull'apparecchiatura terminale prima di essere raccolte.

63. Nel contesto della raccolta di «identificatori unici» su siti web o applicazioni mobili, l'entità che effettua la raccolta sta istruendo il browser (attraverso la distribuzione di codice lato client) a inviare tali informazioni. In quanto tale, è in corso un «accesso» e si applica l'articolo 5, paragrafo 3, della direttiva e-privacy.