Smart Glasses e *privacy* tra Francia e Italia. *Best practices* per le aziende

28/05/2026 PROTEZIONE DEI DATI E CYBERSECURITY, IT&TMT, SOCIETÀ

Roberto A. Jacchia
Camillo Campli
Adriano Garofalo
Marco Stillo

In data 11 maggio 2026, la *Commission Nationale de l'Informatique et des Libertés (CNIL) francese*[1] *ha lanciato un piano d'azione per far fronte agli interrogativi* tanto etici quanto legali connessi all'affermarsi dei dispositivi indossabili intelligenti, e in particolare dei c.d. "smart glasses".

Il piano d'azione trova la sua *ratio* nei risultati del sondaggio *online* svoltosi dal 22 al 29 gennaio 2026, che ha evidenziato diverse preoccupazioni espresse dagli *stakeholders* in merito al funzionamento degli smart glasses. A differenza di uno *smartphone*, che di regola deve essere estratto dalla tasca o dalla borsa per poter essere utilizzato, gli smart glasses contengono dei sensori all'interno della montatura che possono registrare informazioni ambientali, inclusi flussi video del campo visivo dell'utente, registrazioni audio e dati di localizzazione, senza che le persone riprese o registrate ne siano necessariamente consapevoli. Gli smart glasses, inoltre, sono spesso collegati anche ad un sistema di intelligenza artificiale (IA), che consente a chi li indossa di porre domande ad una *chatbot* ed utilizzare le funzionalità del telefono, alcune delle quali possono essere attivate tramite un semplice comando vocale.

Gli smart glasses non sono semplici strumenti tecnologici. Grazie alla loro capacità di acquisire, elaborare e interpretare dati in tempo reale senza che le persone circostanti ne siano necessariamente consapevoli, presentano rischi significativi per la *privacy* e la protezione dei dati personali. Nello specifico, gli smart glasses sono in

[1] La CNIL è l'autorità amministrativa indipendente francese responsabile della protezione dei dati personali.

grado di captare suoni, immagini e video delle persone che si trovano nelle vicinanze dell'utente, e non essendo distinguibili dagli occhiali tradizionali, è molto difficile per le persone vicine capire se vengano riprese o registrate. I dispositivi tecnici che consentirebbero di informare le persone di una registrazione, come ad esempio l'accensione di una spia luminosa, inoltre, hanno una portata limitata o sono, addirittura, assenti.

Facilitando la raccolta di dati tramite un oggetto "non sospetto" di uso quotidiano che, di solito, non ha tale finalità, questi dispositivi presentano un carattere particolarmente invasivo. A differenza di un cellulare, che bisogna estrarre ed orientare, e che vede solo ciò che chi lo indossa gli mostra, gli smart glasses riprendono tutto ciò che ricade nel campo visivo di chi li indossa, con un rischio significativo di non venire identificati come connessi. Ciò che, a sua volta, potrebbe comportare un ulteriore rischio di sorveglianza generalizzata ed una sorta di "normalizzazione" della stessa, in quanto chiunque potrebbe potenzialmente essere dotato di una telecamera in tutti gli spazi pubblici e privati.

Muovendo da queste premesse, la CNIL ha deciso di avviare dei lavori sulla conformità degli smart glasses alla normativa di protezione dei dati personali discutendo con le sue controparti europee in seno al Comitato europeo per la protezione dei dati nonché dialogando con le altre autorità pubbliche competenti in materia. Nel frattempo, la CNIL ha raccomandato agli utenti di i) informare le persone vicine quando utilizzano gli smart glasses, ii) disattivare le funzioni di acquisizione non appena non sono più necessarie, iii) spegnere gli occhiali ogni volta che viene chiesto loro di spegnere il cellulare, iv) evitare di utilizzarli in luoghi dove le persone non se lo aspettano, iv) assicurarsi di ottenere il loro consenso se desiderano utilizzare foto o video in cui compaiono, e vi) riflettere prima di condividere le immagini o i video acquisiti.

Anche in Italia gli smart glasses sono stati oggetto di attenzione. Più particolarmente, nel 2025 il Garante per la protezione dei dati personali aveva avviato un'istruttoria al fine di verificare la conformità del trattamento effettuato da Meta tramite i suoi smart glasses alla normativa vigente in materia, ciò che aveva reso necessario stabilire, da un lato, se essi fossero qualificabili come dispositivi c.d. "IoT"[2] e, dall'altro, se le asserite violazioni fossero riferibili alla sola Direttiva ePrivacy[3] ovvero anche al Regolamento generale sulla protezione dei dati (*General Data Protection Regulation*, GDPR)[4]. Il procedimento, tuttavia, si era poi concluso con l'annullamento d'ufficio del provvedimento sanzionatorio inizialmente prospettato per Meta per superamento dei termini procedimentali dovuto alla straordinaria complessità dell'istruttoria.

Sebbene i promotori di questi dispositivi ne sottolineino l'utilità, e il contributo al progresso in materia di traduzioni istantanee, la loro diffusione non dovrebbe avvenire a scapito dei diritti e delle libertà fondamentali. Qualsiasi azienda che intenda introdurre smart glasses nei propri processi deve preliminarmente svolgere una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) ai sensi del GDPR[5]. Sono

[2] Per IoT (*Internet of Things*) si intende una rete di dispositivi fisici, veicoli, apparecchi e altri oggetti incorporati con sensori, *software* e connettività che consentono di raccogliere e condividere dati.
[3] 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, *GUUE L 201 del 31.07.2002.*
[4] 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, *GUUE L 119 del 04.05.2016.*
[5] L'articolo 35 GDPR, intitolato "Valutazione d'impatto sulla protezione dei dati", ai paragrafi 1-3 dispone: "*... Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie,*

in primo luogo i titolari del trattamento, e in parte i responsabili, a dover valutare l'impatto di qualsiasi operazione che utilizzi smart glasses per il trattamento di dati personali, indipendentemente dal fatto che una DPIA sia o meno legalmente obbligatoria. A tale riguardo, non è sufficiente che un dipendente firmi un consenso generico, in quanto l'azienda deve dimostrare che l'uso degli occhiali è l'unico modo possibile per raggiungere un obiettivo legittimo, come la sicurezza sul lavoro in ambienti pericolosi o la formazione tecnica specialistica.

Il Garante esprime preoccupazione riguarda alla prospettiva che, attratte dalle promesse di maggiore produttività e facilità di accesso alle informazioni, le aziende trascurino di aggiornare le proprie policy sull'uso dei dispositivi personali o aziendali. Nello specifico, non si tratta solo di vietare o consentire l'uso degli occhiali, e bensì di definire confini chiari in merito, tra le altre cose, a dove sia permesso indossarli o ai momenti in cui la funzione di registrazione debba essere disattivata. Le aziende più avvedute, ad esempio, stanno adottando la soluzione delle c.d. "zone libere da registrazioni", mappando i propri uffici definendo aree dove gli smart glasses devono essere obbligatoriamente spenti o riposti[6].

Le analisi tecniche, infine, hanno mostrato che, per funzionare, l'assistente IA degli occhiali richiede il trasferimento continuo di dati verso l'infrastruttura cloud del produttore. La conseguenza è che la percezione di controllo dell'utente collide con una realtà tecnica molto più complessa, in cui l'elaborazione remota dei dati diventa una condizione necessaria per il funzionamento stesso del servizio. Le aziende che adottano smart glasses dotati di IA, pertanto, dovranno mappare l'intera catena del trattamento, individuandone i responsabili ai sensi del GDPR[7] e verificando la sussistenza delle garanzie

considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico...".

[6] Quali bagni, aree relax, sale per colloqui sindacali o uffici dove si discutono strategie confidenziali.

[7] L'articolo 28 GDPR, intitolato "Responsabile del trattamento", ai paragrafi 1-3 dispone: "*... Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.*
Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

adeguate per i trasferimenti verso Stati terzi.

Le iniziative della CNIL e del Garante italiano evidenziano la necessità di promuovere non solo la consapevolezza, da parte degli utenti, del valore dei propri dati, e bensì anche la comprensione, da parte delle aziende, di come la protezione dei dati rappresenti un fattore competitivo e reputazionale strategico, rendendo la tecnica alleata, anziché nemica, delle libertà. Quando un dipendente indossa smart glasses in un luogo pubblico o aperto al pubblico e si guarda intorno, “trasforma” ogni persona che incontra in un soggetto di dati involontario. In assenza di idonee garanzie, chi autorizza l'uso di questi dispositivi si espone a rischi sanzionatori, oltre che risarcitori non solo verso i propri dipendenti, ma verso chiunque entri nel loro raggio d’azione. Il quadro normativo fornisce già oggi una struttura di riferimento robusta. La sfida per le aziende è produrre delle legittime prassi operative, quali DPIA approfondite, policy interne chiare, trasparenza verso tutti i soggetti coinvolti, sicurezza informatica adeguata e governo dell'intera catena del trattamento.

---

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32;
d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati...”.

Roberto A. Jacchia

PARTNER

r.jacchia@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

Camillo Campli

ASSOCIATE

c.campli@dejalex.com
+39 06 809154.1
Via Vincenzo Bellini 24
00198 - Roma

Adriano Garofalo

ASSOCIATE

a.garofalo@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

Marco Stillo

ASSOCIATE

m.stillo@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Potapovsky Lane, 5, build. 2, 4th floor, office 401/12/9 · 101000, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com