Daniele De Paoli

PSD2 e privacy

Sommario: 1. Il problematico disallineamento della disciplina Privacy e PSD2 – 2. Le novità del GDPR e possibili soluzioni per un migliore coordinamento – 3. La centralità della sicurezza e la nuova disciplina dei '*data breach*' – 4. I primi riscontri empirici e riflessioni conclusive.

1. *Il problematico disallineamento della disciplina Privacy e PSD2*

Il Garante per la Protezione dei Dati Personali è impegnato in questo periodo nella complessa fase di implementazione delle nuove norme europee, più faticosa del previsto anche per i fenomeni di disallineamento delle molteplici normative, fra cui quella riguardante la Direttiva PSD2 (Dir. 2015/2366), già trattati dai relatori intervenuti prima di me.

La questione è stata affrontata anche dal Coordinamento delle Autorità europee, che ha operato nel tentativo di superare le difficoltà che si incontrano nella lettura di alcune disposizioni della Direttiva PSD2 in rapporto con il Regolamento UE 2016/679 (c.d. GDPR), dal 25 maggio pienamente efficace.

Pensiamo ad esempio ad alcune 'scivolate', come la definizione dei dati implicati nelle operazioni di pagamento come dati di tipo 'sensibile', che è sicuramente un errore dal punto di vista giuridico, e che dimostra l'assenza di dialogo fra parti importanti dell'apparato comunitario.

Altro elemento di possibile confusione è quello relativo al consenso. Qui è opportuno distinguere tra consenso contrattuale, che è dovuto e previsto, e c.d. consenso privacy, che non sarebbe necessario in situazioni di trattamento nelle quali sono in gioco dati che possono essere trattati dai vari titolari del trattamento anche sulla base della clausola del c.d. legittimo interesse del titolare del trattamento, previsto dal nuovo Regolamento all'art. 6, par. 1, lett. f).

È interessante ricordare come l'Autorità sia venuta a conoscenza, meno

* Il presente scritto, pur rivisto dall'autore, conserva il carattere colloquiale dell'intervento originale al convegno.

di un anno fa, di questo problema del disallineamento. Il tema è stato posto al Garante dall'ABI che aveva la necessità di informare gli associati in merito alle nuove disposizioni (se chiedere un altro consenso, se e come aggiornare le informative ecc.). Ma tutto questo è avvenuto mentre in modo affrettato si stava concludendo il percorso di recepimento italiano della Direttiva PSD2, tanto che le sollecitazioni dell'ABI al Garante sono arrivate lo stesso giorno in cui veniva adottato il Decreto di recepimento della PSD2.

Come Autorità, in questo contesto, non potevamo fare molto. Abbiamo comunque interessato la Presidenza del Consiglio e il MEF e abbiamo fatto capire che sarebbe stato importante ridiscutere sui vari tavoli competenti il tema giustamente posto dagli operatori.

È utile sottolineare che la vicenda del disallineamento, in ambito italiano, è avvenuto in vigenza del Codice privacy del 2003.

In tale quadro normativo l'Autorità Garante aveva il potere di esprimere pareri - obbligatori anche se non vincolanti - solo rispetto alla normazione secondaria (regolamenti, decreti ministeriali, ecc.).

2. *Le novità del GDPR e possibili soluzioni per un migliore coordinamento*

Una significativa novità, che sottolineo per indicare un orizzonte nuovo che si apre per l'Autorità, è data dal fatto che le nuove norme prevedono l'interlocuzione con il Garante anche in fase di produzione di fonti primarie. Quindi un rapporto con il Parlamento, o con il Governo nel momento in cui elabora, ad esempio, decreti legislativi, molto più intenso e articolato di quanto avvenuto finora. Tutto ciò dovrebbe permettere di meglio 'costruire' la normativa, soprattutto quando ci troviamo in presenza di plessi normativi complessi, intersecati con altre normative (proprio come nel caso della PSD2).

Ovviamente sono disposizioni che stanno vivendo le prime settimane di applicazione, come vediamo rispetto a due situazioni in fase di elaborazione normativa e finite in questi giorni al centro dell'attenzione mediatica.

Parlo, da un lato, del progetto legislativo che mira ad introdurre forme più incisive di controllo per i lavoratori pubblici, riguardo alla loro presenza sui posti di lavoro, attraverso l'utilizzo anche di dati di tipo biometrico, dall'altro della generalizzazione dell'utilizzo della videosorveglianza negli asili nido e nelle case di cura.

Tornando al nostro tema, al di là dei problemi interpretativi, mi concentrerei sugli aspetti della disciplina privacy del nuovo Regolamento

che possono incidere ed essere interessanti per verificare l'azione che gli attori di questa catena complessa della PSD2 (banche, nuovi operatori dei sistemi di pagamenti, intermediari vari, ecc.) si troveranno ad intraprendere.

3. *La centralità della sicurezza e la nuova disciplina dei* 'data breach'

L'elemento centrale al quale noi presteremo particolare attenzione è sicuramente l'elemento della 'sicurezza'. Sono in gioco grandi quantità di dati, dati che coinvolgono pesantemente le persone, il portafoglio delle persone, perché - come ha precisato il dottor Meli - le banche devono aprire i conti correnti dei propri clienti. Questa espressione corrisponde a quello che realmente si verifica e che dovrà necessariamente avvenire con una serie di presidi di sicurezza adeguati, tali da impedire che non si apra il conto di fronte a chi non è il titolare o comunque colui che esprime la volontà di avvalersi di quel servizio.

Questa è una tipica problematica di sicurezza e non a caso è uno dei perni su cui ruota il Regolamento. Anche la magica parola *accountability* – responsabilizzazione - di fatto si declina in una sequenza di domande del tipo: sono in grado nel momento in cui tratto dati così delicati, così significativi, di garantire un livello di sicurezza che limiti il più possibile *hackeraggi*, interventi illeciti interni o esterni, non danneggi il cliente, non comporti un danno d'immagine ecc.?

La tradizione precedente della disciplina di protezione dati si è basata, per quanto riguarda le misure di sicurezza, nell'esperienza italiana, sul rispetto delle indicazioni contenute nel famoso Allegato B annesso al Codice privacy che fissava le 'misure minime' di sicurezza che il titolare del trattamento doveva adottare, almeno per non incorrere in sanzioni penali. Mediamente il titolare del trattamento si accontentava di questo.

Questo meccanismo è stato in passato criticato, anche perché mai aggiornato nel corso degli ultimi 15 anni, ma aveva ovviamente una sua praticità di utilizzo: dato un set minimo di misure, le applico e sono tranquillo.

Adesso, se ci riferiamo all'art. 32 del Regolamento europeo sulla sicurezza, il terreno comincia a mancare, perché il riferimento è fatto a categorie assolutamente generali: l'adeguatezza, l'aggiornamento, lo stato dell'arte, la verifica della resilienza dei sistemi, ecc..

Cosa significa questo, in concreto, nel mondo dei nuovi servizi di pagamento? A che punto posso considerarmi in regola?

Questa è la frontiera sulla quale ognuno si trova per evitare il rischio del *data breach* (art. 33), cioè la violazione dei dati personali.

4. *I primi riscontri empirici e riflessioni conclusive*

Al riguardo, abbiamo i primi dati delle denunce di *data breach* fatte a 4-5 mesi dall'adozione delle nuove regole.

In precedenza, la segnalazione delle violazioni di dati personali non era presente nella legislazione italiana, più precisamente l'obbligo gravava, per effetto di un'altra disposizione comunitaria, solo sulle imprese di telecomunicazione.

Il Regolamento generalizza l'obbligo di denuncia dei casi di violazione dei dati personali a tutti i titolari del trattamento.

Sono arrivate finora 400 segnalazioni.

C'è un po' di tutto (*hackeraggi*, furti di *devices* o altri strumenti contenenti dati personali, errori umani). Teniamo presente che circa un anno fa, in era pre-GDPR, uno dei più grossi gruppi bancari italiani ci aveva segnalato una violazione di dati che, partita da un'ipotesi di perdita dati di circa 200 mila correntisti, fortunatamente solo dati anagrafici, in realtà, completate le verifiche, si era estesa fino ad un totale di 700.000 soggetti. E, cosa interessante, il buco non si era verificato nel perimetro interno dell'istituto di credito interessato, ma presso una società esterna responsabile del trattamento, alla quale erano stati affidati incarichi tutto sommato abbastanza limitati. A causa della debole struttura informatica di questo soggetto, si è però aperta una 'porta' (informatica) che ha determinato la fuoriuscita delle informazioni.

Questa è una situazione che segnalo perché, rispetto all'aspetto sicuramente positivo dell'ingresso di nuovi soggetti e dell'offerta di nuove possibilità previste dalla PSD2, con questa realtà dobbiamo fare i conti. Se è già difficile controllare soggetti più strutturati, più tradizionalmente abituati ad avere cura dei propri dati come sono le banche, sicuramente l'attenzione deve essere moltiplicata nei confronti di soggetti nuovi che entrano su questo mercato, magari senza adeguate cautele.

A margine del discorso sui *data breach* possiamo poi ricordare una tematica che nel campo dei dati finanziari è estremamente rilevante, quella dei furti di identità. Un tema di cui nessuno ama parlare perché nessuno vuole ammettere che sono stati persi dati con i quali si sono sottoscritti

contratti, ecc. La casistica è però tuttora diffusa soprattutto nell'ambito del credito al consumo.

Un altro tema sul quale bisognerà maturare riflessioni ed esperienza è il modo col quale il trattamento dei dati da parte degli attori, anche nuovi, si rapporterà all'esercizio dei diritti degli interessati. Su questo punto particolare attenzione va prestata al nuovo diritto alla portabilità dei dati personali che apre nuove prospettive per gli interessati anche nella logica di favorire il passaggio da un operatore ad un altro in chiave anticoncorrenziale.

Vi ringrazio per l'attenzione.

Abstract

Nel breve intervento sono stati sottolineati innanzitutto alcuni aspetti che evidenziano il disallineamento (almeno a livello terminologico) fra la Direttiva PSD2 ed il coevo Regolamento generale sulla protezione dei dati (GDPR). Situazione già rilevata dalle Autorità europee di protezione dei dati, specie con riferimento all'uso improprio della categoria del consenso.

In chiave applicativa, si evidenzia poi come la principale preoccupazione sia quella di assicurare un'alta qualità dei dati trattati, in un contesto in cui occorre soprattutto prevenire i furti di identità ed evitare le perdite (dolose o colpose) di dati. Il nuovo Regolamento europeo pone infatti particolare attenzione alla prevenzione dei rischi dei c.d. data breach.

Parole chiave: Regolamento generale sulla protezione dei dati, GDPR, PSD2, Consenso, Violazione dei dati personali, Data breach, Privacy, Sicurezza dei dati.

Abstract

The short speech analyses some aspects that highlight the misalignment (at least at the terminological level) between the PSD2 directive and the General Data Protection Regulation (GDPR), already addressed by the European Data Protection Authorities, with specific reference to the use of the notion of consent. From a practical point of view, it highlights the main concern of the Authority: ensuring the high quality of the processed data, while preventing the identity theft and the loss of data due to fraud or negligence. The new European Regulation pays particular attention to the prevention of the risks of the so-called data breach.

Keywords: General data protection regulation, GDPR, PSD2, Consent, Personal data breach, Privacy, Data security.