PROTEZIONE DEI DATI PERSONALI: IL RISCHIO DI ABUSI SUI DATI PERSONALI PUÒ COSTITUIRE DANNO IM-MATERIALE

Avv. Silvia Borrini

Capita di frequente che durante questo appuntamento approfondiamo le sentenze emesse dalla Corte di Giustizia dell'Unione Europea (già definita "**CGUE**") che trattino di privacy e di GDPR, apportando interpretazioni con sguardo al futuro a tematiche che pur essendo, all'apparenza se non altro, di patrimonio comune, non sempre sono di immediata comprensione e applicazione.

Il fatto

Veniamo al caso di cui vogliamo discutere.

La sig.ra Vb. riteneva di aver subito un danno immateriale a causa della presunta violazione, da parte dell'Agenzia nazionale per le entrate pubbliche bulgara (di seguito, "**Autorità**"), dei suoi obblighi di legge in quanto titolare del trattamento dei dati personali. Infatti, a seguito di un accesso non autorizzato al sistema informatico dell'Autorità avvenuto il 15.07.2019, taluni dati personali contenuti nel sistema erano stati pubblicati su internet: più di sei milioni di persone fisiche sono state interessate da tali eventi, alcune centinai di esse (tra cui la ricorrente), hanno proposto contro l'Autorità azioni di risarcimento dei danni che sarebbero derivati dalla divulgazione dei loro dati personali.

Nello specifico, il danno immateriale lamentato dalla ricorrente avanti al Tribunale amministrativo statale, consisterebbe nel "timore che i suoi dati personali, pubblicati senza il suo consenso, siano oggetto di un utilizzo abusivo, in futuro, o che essa subisca un ricatto, un'aggressione, o addirittura un rapimento".

L'Autorità, dal canto suo, ha prodotto documenti a dimostrazione del fatto che sono state adottate tutte le misure necessarie, ab origine, per prevenire la violazione dei dati personali contenuti nel suo sistema informatico nonché, da ultimo, per limitare gli effetti di tale violazione. L'Autorità rileva come non si sarebbe configurato alcun nesso causale tra il danno lamentato e la violazione.

Il giudizio di rinvio

Il Giudice di secondo grado chiamato a pronunciarsi sull'impugnazione della sentenza resa dal Tribunale amministrativo che aveva respinto il ricorso della sig.ra Vb., ha ritenuto necessario un intervento della CGUE con riferimento all'interpretazione (i) dell'art. 5, paragrafo 2, (ii) degli articoli 24 e 32 nonché (iii) dell'art. 82, paragrafi da 1 a 3 del Regolamento (UE) 2016/679 ("**GDPR**"). Per l'effetto, rimette la questione alla Corte.

Il giudice del rinvio, considerato che qualora non si ritenga che la sola constatazione della sopravvenienza di una violazione di dati personali sia di per sé evidenza del fatto che le misure attuate dal titolare del trattamento di tali dati non erano "adeguate", ai sensi degli articoli 24 e 32 del RGPD, dovrà valutarsi:

– da un lato, la portata del controllo che i giudici nazionali devono effettuare per valutare l'adeguatezza delle misure di cui trattasi e,
– dall'altro, le norme relative all'assunzione delle prove che devono applicarsi in tale contesto, con riguardo sia all'onere della prova sia ai mezzi di prova, in particolare quando tali giudici sono aditi per un'azione di risarcimento fondata sull'articolo 82 di tale regolamento.

La Corte di appello intende inoltre sapere se, alla luce dell'articolo 82, paragrafo 3, del GDPR, il fatto che la violazione di dati personali risulti da un atto commesso da terzi, nel caso di specie da un attacco informatico, costituisca un fattore che esonera sistematicamente il

titolare del trattamento di tali dati dalla sua responsabilità per il danno causato all'interessato.

Da ultimo, detto giudice si chiede se il timore provato da una persona che i suoi dati personali possano essere oggetto di un utilizzo abusivo in futuro, nel caso di specie a seguito di un accesso non autorizzato agli stessi e della loro divulgazione da parte di criminali informatici, possa, di per sé, costituire un danno immateriale, ai sensi dell'articolo 82, paragrafo 1, del GDPR. In caso affermativo, tale persona sarebbe dispensata dal dimostrare che terzi hanno compiuto, anteriormente alla sua domanda di risarcimento, un uso illecito di tali dati, quale un'usurpazione della sua identità.

L'interpretazione della CGUE

La Corte di Giustizia ha affermato che:

– gli articoli 24 e 32 del GDPR devono essere interpretati nel senso che una divulgazione non autorizzata di dati personali o un accesso non autorizzato a tali dati da parte di "terzi", ai sensi dell'articolo 4, punto 10, di tale regolamento, non sono sufficienti, di per sé, per ritenere che le misure tecniche e organizzative attuate dal titolare del trattamento in questione non fossero adeguate, ai sensi di tali articoli 24 e 32;

– l'articolo 32 del GDPR deve essere interpretato nel senso che l'adeguatezza delle misure tecniche e organizzative attuate dal titolare del trattamento ai sensi di tale articolo deve essere valutata dai giudici nazionali in concreto, tenendo conto dei rischi connessi al trattamento di cui trattasi e valutando se la natura, il contenuto e l'attuazione di tali misure siano adeguati a tali rischi;

– nell'ambito di un'azione di risarcimento fondata sull'articolo 82 di tale regolamento, al titolare del trattamento di cui trattasi incombe l'onere di dimostrare l'adeguatezza delle misure di sicurezza da esso attuate ai sensi dell'articolo 32 di detto regolamento;

– l'articolo 82, paragrafo 3, del GDPR deve essere interpretato nel senso che il titolare del trattamento non può essere esonerato dal suo obbligo di risarcire il danno subito da una persona, ai sensi dell'articolo 82, paragrafi 1 e 2, di tale regolamento, per il solo fatto che tale danno deriva da una divulgazione non autorizzata di dati personali o da un accesso non autorizzato a tali dati da parte di "terzi", ai sensi dell'articolo 4, punto 10, di detto regolamento, dato che tale responsabile deve allora dimostrare che il fatto che ha provocato il danno in questione non gli è in alcun modo imputabile;

– l'articolo 82, paragrafo 1, del GDPR deve essere interpretato nel senso che il timore di un potenziale utilizzo abusivo dei suoi dati personali da parte di terzi che un interessato nutre a seguito di una violazione di tale regolamento può, di per sé, costituire un "danno immateriale", ai sensi di tale disposizione.

Dunque, con la sentenza sulla causa C-340/21 i giudici europei hanno affermato che in caso di divulgazione non autorizzata di dati personali o di accesso non autorizzato a tali dati, i giudici non possono dedurre da questo solo fatto che le misure di sicurezza adottate dal titolare del trattamento non fossero adeguate. Piuttosto, i giudici devono esaminare l'adeguatezza di tali misure in concreto. Il timore di un potenziale utilizzo abusivo dei propri dati personali da parte di terzi, che una persona nutre a seguito di una violazione del GDPR, può di per sé costituire dunque un danno immateriale risarcibile.