"One stop shop": un ostacolo ai poteri delle Autorità di protezione dati e un'opportunità sottovalutata per le autorità giurisdizionali?

Augusta Iannini
Già Vicepresidente Autorità Garante per la protezione dei dati personali, avvocato

L'applicazione effettiva del Regolamento (UE) 2016/679 per il trattamento dei dati transfrontalieri si realizza attraverso il meccanismo dell'"*one stop shop*" (sportello unico) costruito con un insieme di regole che dovrebbero consentire ai titolari ed ai responsabili del trattamento transfrontaliero di dati personali di individuare come punto di riferimento una sola Autorità di controllo.

Questo principio, fortemente perseguito dalle imprese perché doveva semplificare e dare coerenza alle decisioni (anche perché accompagnato dalla straordinaria facoltà – per i titolari del trattamento – di indicare il luogo dello stabilimento principale) ha determinato più di qualche complicazione, non solo per gli interessati (che potrebbero addirittura preferire per la tutela dei loro diritti le autorità giurisdizionali invece che le autorità di protezione dati, in applicazione del principio dell'alternatività dei mezzi di tutela), ma anche per i titolari ed i responsabili del trattamento e, quindi, prevalentemente, per le imprese, non essendo poi così scontata la natura di " dato personale oggetto di trattamento transfrontaliero" e non essendo soprattutto scontata l'adesione ai principi di cooperazione e di coerenza da parte delle Autorità di protezione dati che non si identifichino con quelle nel cui territorio ha sede lo stabilimento principale.

Il principio di territorialità, espresso dall'articolo 5 comma 1, GDPR, consente

ad ogni Autorità di eseguire i compiti assegnati e di esercitare i poteri conferiti in base al Regolamento, nel solo territorio del rispettivo Stato membro (articolo 55, comma 1).
Per i trattamenti" transfrontalieri" – che si verificano quando i dati personali sono trattati nell'ambito delle attività di stabilimenti situati in più di uno Stato Membro da parte di un titolare o responsabile stabiliti in più di uno Stato Membro, ovvero quando i dati sono trattati in un unico stabilimento da parte di un titolare o responsabile nell'Unione ma con incidenza sostanziale su interessati in più di uno Stato Membro – l'autorità competente si identifica nell'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare o del responsabile , con tutte le precisazioni contenute nelle Linee Guida approvate dal Working Party Article 29 il 13 dicembre 2016 e poi emendate ed adottate il 5 aprile 2017.
L' autorità di controllo interessata, in caso di trattamento transfrontaliero di dati personali (articolo 4, punto 22, GRDP) interviene quando:

- il titolare o il responsabile del trattamento è stabilito sul territorio dello Stato Membro di tale autorità di controllo;
- gli interessati -che risiedono nello Stato Membro dell'autorità di controllo- sono o possono essere influenzati in modo sostanziale dal trattamento;
- è stato proposto un reclamo a tale autorità.

Ogni autorità di protezione dati dunque, in base ai criteri sopra indicati, può assumere il ruolo di autorità capofila, di autorità interessata o di mera autorità di controllo (in quest'ultimo caso quando il trattamento dati non ha pacificamente natura transfrontaliera).
La conseguenza delle indicazioni e dei contenuti della definizione di stabilimento principale è il potere riconosciuto dall'articolo 56 comma 6, GDPR, all'autorità capofila di essere l'unico interlocutore del titolare o del responsabile in merito al trattamento transfrontaliero effettuato da tale titolare o responsabile.
Tuttavia, la valutazione dell'incidenza "sostanziale" di un trattamento in più di uno Stati Membri viene valutata caso per caso dalle autorità di controllo interessate, sulla base di specifiche indicazioni quali quelle contenute nel considerando 127, GDPR, per il quale ogni autorità di controllo che non agisca come capofila dovrebbe trattare i casi locali il cui oggetto è rappresentato da uno specifico trattamento che riguarda un singolo Stato Membro e coinvolga soltanto interessati in questo singolo Stato Membro anche se i titolari o i responsabili siano stabiliti in più di uno Stato Membro. Anche nel c.d. "local case", però, l'autorità di controllo informa l'autorità capofila e può subirne l'eventuale richiesta di trattare il caso (articolo 56, par 2,3,4, GDPR),

con la conseguente applicazione, in tale ipotesi, del meccanismo previsto dall'articolo 60, GDPR (cooperazione e coerenza). Ma l'individuazione di cosa caratterizzi il "local case" non è affatto semplice e, in ogni caso e per qualsiasi fattispecie, la tentazione di percorrere delle strade che consentano alle Autorità di protezione dati di riprendersi una fetta di potere attraverso il ricorso alle autorità giudiziarie, in applicazione dell'articolo 58, comma 5, GDPR è forte. Cosicché la Corte di Giustizia (Grande Sezione) con la sentenza del 15 giugno 2021 ha provato a circoscrivere questo potere, ma l'interpretazione proposta appare parzialmente convincente. La questione, per la parte che ci interessa, riguarda le condizioni in presenza delle quali un'autorità nazionale di controllo, priva della qualità di autorità di controllo capofila riguardo ad un trattamento transfrontaliero, possa esercitare il suo potere di intentare un'azione dinanzi ad un giudice di uno Stato Membro per una presunta violazione del Regolamento, in applicazione dell'articolo 58, comma 5.

La Corte, dopo aver esaminato le regole sulla competenza, i doveri di cooperazione , i meccanismi dello sportello unico, ha concluso che, in materia di trattamento transfrontaliero di dati personali, la competenza dell'autorità capofila costituisce la regola, mentre la competenza delle altre autorità di controllo interessate alla decisione costituisce l'eccezione e quindi l'autorità di controllo non capofila può intentare un'azione giudiziale purché ciò "avvenga in una delle situazioni in cui il Regolamento 2016/679 conferisce a tale autorità di controllo la competenza ad adottare una decisione che accerti che il trattamento in questione viola le norme in esso contenute , nonché nel rispetto delle procedure di cooperazione e coerenza previste dal Regolamento". Dunque, come nel gioco dell'oca, la Corte ha rimandato tutto al punto di partenza, eludendo alcuni nodi connessi all'importanza che il controllo indipendente riveste nell'ambito del diritto europeo sulla protezione dati ed alla valenza dell'affermazione contenuta nel considerando 122 del Regolamento per il quale " ogni autorità di controllo dovrebbe avere la competenza, nel territorio del proprio Stato Membro, ad esercitare i poteri e ad assolvere i compiti ad essa attribuiti a norma del regolamento medesimo" con la conseguenza che un meccanismo procedurale come quello dell'"one-stop-shop" non dovrebbe ridurre i poteri delle autorità nazionali di ricorrere dinanzi alle autorità giurisdizionali in applicazione dell'articolo 58, comma 5, GDPR, che non sembra peraltro prevedere forme di " autocensura" dei poteri dell'autorità di controllo.

L'interrogativo sulla "competitività" del ricorso alle autorità giurisdizionali rispetto alle autorità di protezione dati si pone non solo in relazione al potere di queste autorità di ricorrere alle autorità giurisdizionali ma

anche rispetto all'eventuale opposizione degli interessati alla decisione di un'autorità capofila e, soprattutto, rispetto alla facoltà che il Regolamento riconosce ai titolari ed agli interessati di scegliere, per la tutela dei propri diritti, un'autorità giurisdizionale rispetto ad un'autorità di protezione dati, in virtù del principio di alternatività della tutela riconosciuto dall'articolo 79 del Regolamento, applicabile anche in caso di trattamento transfrontaliero di dati personali. Nel meccanismo dell'"one-stop-shop", l'autorità capofila ha certamente un ruolo importante di guida e coordinamento delle altre autorità interessate; è comunque colei che emana l'unica decisione finale, pur dovendo interpellare tutte le autorità interessate prima di assumere un qualsiasi provvedimento nei confronti del titolare o del responsabile del trattamento. Ma nella complessa procedura instaurata tra autorità di controllo interessata e autorità capofila, magari con l'intervento del Comitato Europeo per la Protezione Dati, l'Autorità capofila, in caso di archiviazione o di rigetto di un reclamo, deve rivolgersi all'autorità di controllo dinanzi alla quale è stato proposto il reclamo perché faccia propria la decisione, la notifichi al reclamante e ne informi il titolare del trattamento. Scopo di questa procedura è proprio quello di individuare l'autorità giurisdizionale dinanzi alla quale si potrà presentare opposizione, autorità che sarà appunto quella dinanzi alla quale l'interessato ha proposto la sua istanza e/o il suo reclamo: in sede di eventuale opposizione dunque, la decisione nel merito "definitiva" sarà espressa dall'autorità giudiziaria, che recupera in questa fase un ruolo assai più significativo rispetto all'autorità di protezione dati interessata che, magari ,quella decisione ha dovuto subire a causa del meccanismo dello sportello unico.

E allora perché non anticipare la tutela privilegiando da subito le autorità giurisdizionali del proprio Stato Membro, anche in caso di trattamento transfrontaliero dei dati personali?

Inoltre, poiché la tutela dei diritti dei titolari e degli interessati per le violazioni del Regolamento, anche nell'ipotesi di trattamento transfrontaliero di dati personali, può essere esercitata "ab origine" (grazie al principio dell'alternatività della tutela) dinanzi alle autorità giurisdizionali dello Stato Membro in cui il titolare o il responsabile hanno uno stabilimento oppure dinanzi alle autorità giurisdizionali dello Stato Membro in cui l'interessato risieda abitualmente (tranne il caso in cui titolare o responsabile sia un'autorità pubblica di uno Stato Membro nell'esercizio dei pubblici poteri), le maggiori opportunità offerte dalle decisioni di tali autorità potrebbero essere ancora più apprezzate.

L'azione infatti si pone come un'ordinaria azione civile diretta o ad ottenere la cessazione della condotta lesiva del titolare o del responsabile oppure

– ed eventualmente anche congiuntamente – il risarcimento del danno da parte del titolare o del responsabile (possibilità quest'ultima sicuramente esclusa per le autorità di protezione dati dal nostro ordinamento): le relative azioni legali sono promosse dinanzi alle autorità giurisdizionali competenti secondo le regole descritte nell'articolo 79, comma 2, GDPR (foro dello Stato Membro in cui il titolare o il responsabile ha uno stabilimento, foro dello Stato Membro in cui l'interessato risiede abitualmente con l'eccezione del foro obbligatorio dello Stato Membro in cui si trova l'Autorità pubblica nell'esercizio dei pubblici poteri ,titolare o responsabile del trattamento); regole sicuramente più consolidate rispetto a quelle fissate nella procedura dell'"one-stop- shop".

Gli opportuni richiami operati dal considerando 147 alle regole di giurisdizione contenute nel Regolamento privacy ed al "suggerimento" che queste regole, in particolare quelle che riguardano i procedimenti giurisdizionali nei confronti dei titolari o responsabili del trattamento, anche per risarcimento del danno, siano considerate "speciali" rispetto alle disposizioni generali in materia di giurisdizione contenute nel Regolamento UE 1215/2012, non consentono comunque di apprezzare il meccanismo dell'"one-stop-shop" – per nulla chiarito dall'interpretazione della sentenza della Corte di Giustizia -mentre la limitazione dei contenuti delle decisioni delle Autorità di protezione dati – sotto l'aspetto risarcitorio – rispetto a quelli delle Autorità giurisdizionali rischia di rendere più "appetibile" per gli interessati il ricorso a queste autorità.

Ne consegue che i vantaggi di un ricorso alle autorità di protezione dati dei singoli Stati Membri rischiano di essere confinati a quei casi di minore importanza che possono vantare una maggiore rapidità dei tempi di definizione ma che non potranno avere in ogni caso (almeno per il nostro ordinamento) contenuti risarcitori.

Per tutte queste considerazioni appare sempre più doveroso, a seconda del caso concreto, riflettere sulle migliori strategie "processuali" da percorrere per tutelare al meglio i diritti dei soggetti lesi da trattamenti illeciti dei loro dati personali.