

IL DIFFICILE EQUILIBRIO TRA CONSENSO DELLA PERSONA INTERESSATA
E LEGITTIMO INTERESSE DEL TITOLARE DEL TRATTAMENTO: PROBLEMI
E PROSPETTIVE NEI RAPPORTI TRA FONTI INTERNE E DELL'UNIONE
EUROPEA IN TEMA DI TUTELA DEI DATI PERSONALI

DAVIDE BALDINI*

Sommario

1. Introduzione. - 2. Il legittimo interesse del titolare all'interno della direttiva. - 3. Il recepimento dell'articolo 7(f) negli Stati membri. - 4. L'assenza di un orientamento interpretativo consolidato nella giurisprudenza della Corte di giustizia. - 5. Il rapporto tra consenso e legittimo interesse alla luce degli articoli 16 TFUE e 7 e 8 della Carta. - 6. Il potenziale impatto del Regolamento (UE) 2016/679 nel rapporto tra legittimo interesse e consenso. - 7. Osservazioni conclusive.

Abstract

The broad wording of the legal basis of the legitimate interest of the data controller, foreseen by the EU data protection legislation, has fed different approaches in the practice of national data protection authorities. The lack of binding guidance on the relationship with the alternative legal basis of the data subject's consent, coupled with different constitutional traditions on the recognition of privacy and data protection, also contributed to heterogeneity. After providing an in-depth analysis of the current state of the practice, this contribution will examine the impact of Articles 7 and 8 of the EU Charter of fundamental rights on the respective role of the legal bases of the consent of the data subject and the legitimate interest of the data controller. Attention is also paid to the new data protection Regulation, which shall become applicable in May 2018 and may shed some light on the issue.

Suggerimento di citazione

D. BALDINI, *Il difficile equilibrio tra consenso della persona interessata e legittimo interesse del titolare del trattamento: problemi e prospettive nei rapporti tra fonti interne e dell'Unione europea in tema di tutela dei dati personali*, in *Osservatorio sulle fonti*, n. 3/2017. Disponibile in: <http://www.osservatoriosullefonti.it>

* Dottore in Giurisprudenza presso l'Università degli Studi di Firenze.
Contatto: davide.baldini@stud.unifi.it

1. Introduzione

Tra le sei fattispecie stabilite in via alternativa dall'art. 7 della Direttiva 95/46/CE sulla protezione dei dati (di seguito, la "Direttiva")¹ quali basi giuridiche del trattamento di dati personali, la lettera (f) prevede che la presenza di un generico legittimo interesse, vantato dal titolare del trattamento o da un terzo, può fondare la liceità dell'utilizzo di tali dati, a condizione che non prevalgano "l'interesse o i diritti e le libertà fondamentali della persona interessata e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali".² L'ampiezza della formulazione, unitamente alla mancanza di una espressa gerarchia tra le sei basi giuridiche, rendono virtualmente possibile il ricorso all'interesse legittimo del titolare del trattamento – in sostituzione al consenso – in un numero virtualmente illimitato di ipotesi. Diversamente, un problema simile non sussiste – o almeno non nelle stesse proporzioni – per le altre quattro basi giuridiche ulteriori al consenso, che sono state tipizzate dal legislatore.³

L'ampiezza con cui la Direttiva riconosce a un soggetto la possibilità di trattare i dati in presenza di un proprio legittimo interesse al trattamento pone la questione del ruolo del consenso della persona interessata⁴ (di seguito, "l'interessato") nell'ambito delle sei basi giuridiche e più in generale nel diritto dell'Unione in materia di tutela dei dati personali. Evidentemente, maggiore è la portata riconosciuta al legittimo interesse come fondamento di liceità, minore sarà lo spazio riservato al consenso e dunque alla possibilità, per l'individuo, di poter decidere in ordine all'eventualità che un terzo possa trattare o meno i propri dati. L'alternatività della base giuridica del legittimo interesse al consenso⁵ dell'interessato desta pertanto preoccupazioni in chi considera la normativa di protezione dei dati uno strumento che dà attuazione al diritto di ciascun individuo a determinare l'utilizzo che un altro soggetto può fare dei dati personali e in chi vede di conseguenza nell'autodeterminazione dell'interessato il fondamento di liceità principale.⁶

¹ GUUE 1995 L 281, p. 31 ss.

² Combinato disposto degli artt. 7(f) e 1(1) della direttiva.

³ F. FERRETTI, *Data Protection and the Legitimate Interests of Data Controllers: Much Ado About Nothing or the Winter of Rights?*, in *Com. mar. law rev.*, 2014, p. 843 ss., 854-856.

⁴ Ovvero la persona i cui dati personali sono oggetto di trattamento (artt. 2 lett. (a) e (b) della Direttiva).

⁵ Previsto dall'art. 7(a) della Direttiva. Per essere valido, deve essere libero, specifico e informato.

⁶ Ad esempio, F. FERRETTI, *The Winter of Rights?*, cit., p. 866. L'autore propone un'interpretazione correttiva e "rights-oriented" della disposizione, volta a chiarire che il consenso dell'interessato costituisce il fondamento di liceità principale.

Sin dalla fase iniziale del recepimento della Direttiva,⁷ nella dottrina e nella prassi delle autorità di controllo degli Stati membri sono emerse posizioni diverse rispetto ai confini dell'interesse legittimo quale base giuridica del trattamento. All'origine di queste divergenze ci sono questioni che attengono strettamente al rapporto tra la normativa dell'Unione sulla protezione dei dati e i diritti fondamentali al rispetto della vita privata e alla tutela dei dati personali quali riconosciuti, rispettivamente, dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (di seguito, la "Carta"). In primo luogo, la suddetta normativa persegue una duplice finalità, di stampo "mercantilistico" l'una (assicurare la circolazione dei dati) e relativa alla tutela dei diritti fondamentali (assicurare la protezione dei dati) l'altra. Inoltre, le autorità di controllo nazionali istituite dalla stessa Direttiva, a partire dal Garante per la protezione dei dati personali italiano (di seguito il "Garante"),⁸ interpretano l'art. 7, lettera f) alla luce dei principi e criteri spesso derivanti dal diritto costituzionale nazionale: l'esistenza di approcci diversi circa la ricostruzione della natura – sostanziale o procedurale – dei diritti alla *privacy* e alla protezione dei dati personali sfocia, di conseguenza, in approcci difformi delle autorità di controllo.

In questo quadro, lo scopo del presente contributo è quello di esaminare, anche alla luce della giurisprudenza della Corte e delle novità apportate dall'ormai prossima applicabilità del Regolamento (UE) 2016/679,⁹ le prospettive e i problemi posti dalla presenza del legittimo interesse del titolare tra le basi giuridiche del trattamento dei dati personali, con particolare riguardo alle ricadute, sul piano dei rapporti tra diritto UE e nazionale, di una eventuale riconduzione a unità, da parte della Corte di Giustizia, degli approcci divergenti attualmente alimentati dalle autorità garanti nazionali.

2. Il legittimo interesse del titolare all'interno della direttiva

Se nell'ambito degli ordinamenti nazionali le normative a tutela dei dati personali nascono con lo scopo di salvaguardare il diritto fondamentale al rispetto della vita privata dai pericoli derivanti dallo sviluppo della tecnologia informatica, alla base dell'adozione della Direttiva vi è anche un'ulteriore ragione. È infatti proprio a causa del fiorire, nel corso degli anni Settanta e Ottanta, di normative nazionali degli Stati membri poste a protezione dei dati personali e, dunque, in risposta al conseguente rischio di frammentazione regolatoria in un settore già all'epoca di grande importanza economica, che ver-

⁷ COM(2003) 265 final, "First report on the implementation of the data protection directive (95/46/EC)," Brussels, 15.5.2003.

⁸ Art. 153 d.lgs. 196/2003.

⁹ GUUE 2016 L 119, p. 1 ss. Il Regolamento è entrato in vigore il 25 maggio 2016 ma la sua applicabilità è sospesa per due anni a causa dei rilevantissimi cambiamenti apportati.

rà adottata la Direttiva nel 1995. In questa fase, la giustificazione del ravvicinamento legislativo in questo ambito è pertanto da ricercarsi nell'obiettivo di stabilire una libera circolazione dei dati personali tra gli Stati membri; la base giuridica utilizzata per adottare la Direttiva, cioè l'art. 114 TFUE, legittima infatti l'Unione ad adottare atti diretti a perseguire "l'instaurazione ed il funzionamento del mercato interno".

Allo stesso tempo, a fronte di questo fine di carattere mercantilistico, "la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali" è una finalità fin da subito affermata dall'art. 1(1) della Direttiva. Mentre il primo obiettivo è l'unico a trovare, almeno inizialmente, riconoscimento nel diritto primario, l'obiettivo di salvaguardare i diritti fondamentali resta in questa fase confinato al diritto derivato. Una parificazione delle due finalità si è avuta solo a seguito dell'entrata in vigore del Trattato di Lisbona, con l'inserimento nei Trattati dell'art. 16 TFUE¹⁰. Questo articolo racchiude, infatti, in un'unica base giuridica sia la finalità di dare attuazione al diritto fondamentale alla protezione dei dati, sia quella di stabilire una circolazione dei dati libera tra gli Stati membri.

Occorre tenere in considerazione il duplice fondamento della protezione dei dati all'interno del diritto dell'Unione nell'esame delle questioni poste dall'art. 7, dal momento che la stessa struttura della Direttiva e la sua interpretazione da parte della Corte sono influenzate da questa dualità di scopi.¹¹

L'obiettivo di tutela dei diritti fondamentali è riflesso nelle caratteristiche essenziali della Direttiva, a partire dalla tassatività delle sei ipotesi in cui viene legittimato il trattamento di dati personali, che fa assumere un carattere generalmente proibitivo alla possibilità di trattare dati personali, ulteriormente rafforzato nel caso in cui si abbiano ad oggetto dati sensibili.¹² Lo stesso può dirsi per le prescrizioni normative che si applicano in corso di trattamento e che costituiscono la "spina dorsale" della normativa: i principi relativi alla qualità dei dati, i diritti dell'interessato e le disposizioni volte a limitare il trasferimento di dati verso quei paesi terzi che non attribuiscono un livello di

¹⁰ Considerazioni equivalenti in ordine al fondamento giuridico si possono fare per quanto riguarda la Direttiva 2002/58/CE (GUUE 2002 L 201, p. 37 ss.) cd. sull'*e-privacy*, che costituisce *lex specialis* nei confronti della Direttiva 95/46, essendo diretta a regolare unicamente quei trattamenti di dati che avvengono nell'ambito delle comunicazioni elettroniche. La Direttiva del 2002 condivide infatti con la 95/46 la medesima base giuridica, vale a dire l'art. 114 TFUE. Tuttavia, in essa la questione oggetto di esame è stata risolta espressamente dal legislatore a favore del consenso, dal momento l'utilizzabilità dell'interesse legittimo viene prevista unicamente in ipotesi predeterminate.

¹¹ *Infra*, par. 4; O. LYNSKEY, *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, I ed., 2015.

¹² *Cfr.* art. 8 della Direttiva.

tutela adeguato ai dati personali. Tutti questi elementi concorrono a determinare un elevato livello di tutela dei diritti fondamentali dell'interessato.¹³

A ben vedere, l'attribuzione di un simile livello di tutela, anziché porsi in contrasto con l'obiettivo mercantilistico, risulta funzionale al suo raggiungimento, come riconosciuto dal considerando 9 della Direttiva, dal momento che impedisce agli Stati membri di frapporre ostacoli normativi al flusso transfrontaliero di dati verso un altro Stato dell'Unione, sul presupposto che un tale Paese non attribuisca una protezione adeguata ai dati personali. Invero, i due obiettivi alla base della Direttiva, piuttosto che in tensione, risultano strettamente correlati tra di loro, dal momento che l'obiettivo mercantilistico può essere raggiunto soltanto mediante l'attribuzione di un elevato livello di protezione ai diritti umani.

Tuttavia, è proprio nell'ambito del carattere generalmente proibitivo del trattamento disegnato dall'art. 7 della Direttiva che i due scopi entrano in tensione tra di loro. L'art. 7(f) ha infatti trovato una vasta applicazione, in alcuni Stati membri, per fondare la liceità di trattamenti di dati personali da parte di soggetti privati per finalità economico-commerciali, quali, a titolo di esempio, la profilazione¹⁴ per finalità di *marketing*, operazioni di *data analytics* sui *big data*, *data mining*, incrocio di banche dati e via discorrendo.¹⁵ La possibilità di avvalersi di un proprio interesse commerciale a trattare i dati, senza dover previamente ottenere un valido consenso da parte dell'interessato, agevola in modo significativo gli operatori economici che trattano dati personali nello svolgimento delle proprie attività.¹⁶ Quest'ultima base giuridica costituisce infatti un adempimento che può rivelarsi particolarmente gravoso,¹⁷ e sovente impraticabile,¹⁸ in particolare a causa dei requisiti stabiliti dall'art.

¹³ Cfr. rispettivamente artt. 6, 10-15, 25-26.

¹⁴ Il nuovo Regolamento, all'art. 4 n. 4) definisce come profilazione "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica."

¹⁵ Andando ben oltre le finalità gestionali o di *marketing* indicate dal considerando 30 come idonee ad essere legittimate dalla disposizione. F. FERRETTI, *The Winter of Rights?*, cit., p. 857.

¹⁶ P. BALBONI ET AL., *Legitimate interest of the data controller. New data protection paradigm: legitimacy grounded on appropriate protection*, in *International Data Privacy Law*, 2013, p. 244 ss.

¹⁷ F. FERRETTI, *The Winter of Rights?*, cit., p. 856.

¹⁸ Specialmente nei casi di trattamenti effettuati utilizzando nuove tecnologie, che per il loro stesso funzionamento mal si conciliano con l'ottenimento di un valido consenso. Allo stesso modo, le altre basi, o perché tipizzano fattispecie troppo ristrette (lett. b e d), o perché sotto il profilo soggettivo si applicano soltanto o principalmente ad autorità pubbliche (lett. c ed e), non appaiono idonee a legittimare simili modalità di trattamento, nei casi in cui la finalità di queste sia il perseguimento di interessi di carattere economico da parte di soggetti privati (H. URSIC, B. CUSTERS, *Legal Barriers and Enablers to Big Data Reuse*, in *European Data Protection Law Review*, 2016, p. 209 ss.).

2(h) della Direttiva, che escludono la liceità del consenso come mera possibilità di *opt-out*.¹⁹

Per questi motivi, complice l'ampia formulazione, quello sul legittimo interesse è un fondamento di liceità potenzialmente idoneo a legittimare trattamenti di dati personali effettuati da privati per scopi commerciali ed è per questo di importanza strategica per l'industria legata all'economia digitale.²⁰ Tuttavia, proprio perché esso può costituire una base giuridica alternativa al consenso in un vasto e rilevante numero di ipotesi, impedendo all'individuo l'esercizio del diritto di autodeterminare l'impiego che viene fatto dei propri dati personali, l'interpretazione della disposizione sul legittimo interesse si pone al centro della tensione tra l'obiettivo mercantile e quello di tutela dei diritti fondamentali, oggi entrambi riconosciuti, come anticipato, dall'art. 16 TFUE come alla base della normativa sulla protezione dei dati personali.

3. Il recepimento dell'articolo 7(f) negli Stati membri

L'ampia formulazione della base giuridica in esame, unita alla mancanza di indicazioni espresse nella Direttiva circa il rapporto tra consenso e legittimo interesse, ha portato allo sviluppo di due diversi orientamenti nella prassi applicativa delle autorità di controllo e nella giurisprudenza nazionali.

In alcuni ordinamenti, l'art. 7(f) viene ricostruito come norma di carattere eccezionale, al pari delle ipotesi da (b) a (e). In questi casi il consenso è dunque l'autodeterminazione dell'interessato in ordine al trattamento dei dati, si configurano come il fondamento di liceità principale, mentre le fattispecie alternative al consenso, assumendo appunto carattere eccezionale, vengono ricostruite in maniera restrittiva. In alcuni casi, l'utilizzo del legittimo interesse è subordinato a una previa autorizzazione della stessa autorità di controllo, o ancora l'ambito applicativo delle basi giuridiche diverse dal consenso risulta in parte limitato direttamente dalle modalità di recepimento legislativo delle disposizioni.²¹

Un chiaro esempio di tale approccio ostile al legittimo interesse è fornito dall'ordinamento italiano, dove la possibilità di fondare un trattamento di dati su questa disposizione è limitata da restrizioni sia di carattere legislativo sia dalla prassi applicativa del Garante. Quanto al primo aspetto, l'art. 24(g) del D. Lgs. 196/2003 (c.d. Codice Privacy), nel trasporre la fattispecie *ex art. 7(f)* della Direttiva, aggiunge che essa si applica solo "nei casi individuati dal Ga-

¹⁹ Come si vedrà *infra*, par. 6, il nuovo Regolamento rinforza ulteriormente i requisiti del consenso.

²⁰ *Ex multis*: P. BALBONI, *Legitimate interest of the data controller*, cit., p. 251; F. FERRETTI, *The Winter of Rights?*, cit., p. 856.

²¹ P. BALBONI, *Legitimate interest of the data controller*, cit., p. 249-253; F. FERRETTI, *The Winter of Rights?*, cit., p. 855-858; COM(2003) 265 final, cit.

rante sulla base dei principi sanciti dalla legge". La *ratio* di questo meccanismo è chiara: il trattamento in assenza del consenso dell'interessato costituisce un'interferenza con la possibilità per l'individuo di decidere sul trattamento dei propri dati personali; di conseguenza, il bilanciamento tra legittimo interesse del titolare e diritti fondamentali dell'interessato deve essere sottratto all'autovalutazione del primo e affidata a un'autorità indipendente. In altri termini, al di là delle ipotesi tipizzate dalle lettere da (b) ad (e) dell'art. 7 della Direttiva, il carattere giustificato e proporzionale di un trattamento alternativo al consenso viene dunque sottoposto al previo controllo da parte dell'autorità. Nell'ambito di questa attività, il Garante esamina singole richieste,²² ovvero emana provvedimenti di portata più generale, che fondano la liceità di un trattamento finalizzato a perseguire un legittimo interesse per intere categorie di trattamenti.²³ Il Garante è chiaro nel riconoscere al consenso dell'interessato il ruolo di fondamento principale di liceità, mentre le fattispecie alternative rivestono carattere eccezionale.²⁴ Un approccio simile si rinviene nell'ordinamento giuridico tedesco, dove l'interpretazione della disposizione risulta particolarmente restrittiva²⁵ e in parte limitata altresì dalle modalità di recepimento legislativo,²⁶ e anche in Finlandia, Francia, Grecia e Spagna.²⁷

In altri paesi si è invece sviluppato un approccio opposto, secondo cui consenso e legittimo interesse hanno la medesima dignità, al pari delle altre quattro fattispecie.²⁸ Di conseguenza, le autorità garanti interpretano la disposizione sul legittimo interesse in maniera estensiva e il legislatore ha recepito l'art. 7 trasponendo le disposizioni in maniera letterale, senza subordinare l'applicabilità dell'ipotesi *sub(f)* al soddisfacimento di ulteriori requisiti.

L'esempio principale al riguardo è il regime vigente nel Regno Unito, ove le linee-guida adottate dall'*Information Commissioner's Office* (l'autorità ga-

²² Tra i più recenti, si veda il provvedimento n. 199 del 20 aprile 2017, doc. web n. 6407608, ove il Garante ha respinto la richiesta di una compagnia assicurativa relativamente alla creazione di una banca dati contenente informazioni relative a soggetti che abbiano richiesto preventivi per la sostituzione dei vetri delle proprie automobili, al fine di incrociarli con i dati di chi richiede una polizza "cristalli" o denuncia un sinistro di tale tipo.

²³ Tra i più rilevanti vi è il provvedimento generale relativo alla videosorveglianza, n. 99 dell'8 aprile 2010 "Provvedimento in materia di videosorveglianza" doc. web n. 1712680.

²⁴ "Fatte salve alcune eccezioni, per i soggetti privati e gli enti pubblici economici il trattamento di dati personali è possibile con il consenso dell'interessato", <http://www.garanteprivacy.it/home/doveri>.

²⁵ P. BALBONI, *Legitimate interest of the data controller*, cit., p. 253.

²⁶ <https://clientsites.linklaters.com/Clients/dataprotected/Pages/Germany.aspx>, ultimo accesso il 20.10.2017.

²⁷ P. BALBONI, *Legitimate interest of the data controller*, cit., p. 249-253; COM(2003) 265 final, cit., p. 76-77.

²⁸ F. FERRETTI, *The Winter of Rights?*, cit., p. 855.

rante nazionale) considerano espressamente i diversi fondamenti di legittimità del trattamento come aventi un uguale peso.²⁹ L'utilizzo del consenso o del legittimo interesse quale base giuridica dipende dalle circostanze concrete del caso, e l'autorità non esprime alcuna automatica preferenza per il consenso quale fondamento di liceità principale. Lo stesso approccio si riscontra in Irlanda³⁰ e nei Paesi Bassi.³¹

Evidentemente, questo secondo orientamento è molto più favorevole agli interessi delle imprese rispetto al primo: mediante una lettura estensiva dell'art. 7(f) l'ordinamento giuridico attribuisce la titolarità iniziale sui dati personali in capo agli operatori economici, che possono trattare tali informazioni per le proprie (legittime) finalità commerciali senza dover richiedere il previo consenso dell'interessato, che deve talvolta essere ottenuto in ipotesi specifiche.³²

Tra le cause che hanno determinato una tale frammentazione nel diritto vivente degli Stati membri rientra il sistema di rimedi adottato dalla Direttiva, che affida un ruolo di primo piano alle autorità di controllo nazionali in assenza di un efficace meccanismo di coordinamento. Tra i compiti attribuiti alle autorità vi sono, in particolare, quello di vigilare sul rispetto delle disposizioni della Direttiva e quello di ricevere i ricorsi di persone fisiche che ritengono di aver subito violazioni dei propri diritti. A tal fine, le autorità possono irrogare sanzioni e altre misure di carattere repressivo e punitivo nei confronti dei soggetti responsabili delle violazioni.³³ Ad esse è affidata, in altri termini, una funzione di controllo sul rispetto della normativa, mediante l'attribuzione di poteri di natura para-giurisdizionale, in modo simile a quanto avviene ad esempio con le autorità garanti della concorrenza. A livello strutturale, si trat-

²⁹ <https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/>, ultimo accesso il 20.10.2017. "In our view it is better to concentrate on making sure that you treat individuals fairly rather than on obtaining consent in isolation. Consent is the first in the list of conditions for processing set out in the Act, but each condition provides an equally valid basis for processing."

³⁰ <https://www.dataprotection.ie/docs/Data-Protection-Rule-1/y/23.htm>, ultimo accesso il 20.10.2017.

³¹ P. BALBONI, *Legitimate interest of the data controller*, cit., p. 249-250.

³² N. PURTOVA, *Default entitlements in personal data in the proposed Regulation: Informational self-determination off the table... and back on again?*, in *Computer Law & Security Review*, 2014, p. 6 ss.

³³ Pur restando in alternativa possibile ricorrere direttamente all'autorità giudiziaria per le violazioni relative alla protezione dei dati, per la maggiore rapidità decisionale delle autorità le persone interessate prediligono fare ricorso a queste ultime. Si veda in proposito il *report* elaborato dall'Agenzia dell'Unione europea per i diritti fondamentali (FRA), "Data Protection in the European Union: the role of National Data Protection Authorities", 2010, disponibile al *link* <http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities>, ultimo accesso il 20.10.2017.

ta anche in questo caso di autorità amministrative indipendenti, dal momento che la Direttiva attribuisce loro una piena indipendenza dal potere politico.³⁴

Le autorità di controllo si trovano dunque in una posizione peculiare, a metà strada tra diritto interno e diritto dell'Unione: esse sovrintendono l'applicazione pratica della Direttiva, che ne prevede l'istituzione e – in modo generico – le attribuzioni e i poteri, demandandone però, in concreto, al diritto interno la disciplina di dettaglio.³⁵ Questa ambigua collocazione ha portato molte autorità a fare più o meno espressamente riferimento a orientamenti dottrinali o ai principi vigenti nel diritto nazionale, in special modo di rango costituzionale, per fissare un equilibrio tra consenso e interesse legittimo.³⁶ In tal modo, il limite richiamato dallo stesso art. 7(f), nella parte in cui subordina la possibilità di avvalersi del legittimo interesse alla “condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali e particolarmente del diritto alla vita privata con riguardo al trattamento dei dati personali” è stato spesso interpretato in conformità a quanto ricavabile dall'ordinamento costituzionale dello Stato membro di riferimento.³⁷

Il meccanismo di coordinamento tra le autorità di controllo istituito dall'art. 29 della Direttiva non è riuscito a porre rimedio in maniera efficace a questo *trend*. L'attività delle autorità garanti avviene con un grado di cooperazione che non appare più, ad oggi, adeguato alle caratteristiche sempre più transfrontaliere dei trattamenti di dati, alla accresciuta importanza economica degli stessi rispetto al 1995, né ai maggiori pericoli per i diritti fondamentali rappresentati dallo sviluppo e dalla capillare diffusione di Internet, dell'economia digitale e delle nuove tecnologie.³⁸ Il “Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali” (da ora in avanti “Gruppo di Lavoro”), che riunisce i rappresentanti delle autorità di ciascuno Stato membro, non è infatti dotato di effettivi poteri di coordinamento: esso può emanare linee-guida e simili strumenti di *soft law*, ma non dispone di alcun tipo di potere decisorio vincolante.

Non vi è, dunque, all'interno del sistema disegnato dalla Direttiva, alcun meccanismo di coordinamento istituzionalizzato tra le autorità garanti: qualsiasi forma di coordinamento tra le autorità avviene ad un livello orizzontale e

³⁴ Art. 28(1) della Direttiva.

³⁵ H HIJMANS, *The European Union as a constitutional guardian of internet privacy and data protection*, Springer International Publishing, Bruxelles, I. ed., 2016, p. 287.

³⁶ Article 29 Working Party, *Opinion 15/2011 on the definition of consent*, 844/14/EN, p. 7. “Some Member States see [consent] as a preferred ground, sometimes close to a constitutional principle, linked to the status of data protection as a fundamental right. Other Member States may see it as one of six options, an operational requirement that is no more important than the other options.” Per un riassunto delle differenti ricostruzioni dottrinali si veda *infra*, par. 5.

³⁷ F. FERRETTI, *The Winter of Rights?*, cit., p. 855.

³⁸ Si veda ad esempio il considerando 9 del Regolamento.

del tutto informale, incapace di risolvere le divergenze interpretative che inevitabilmente insorgono tra le varie autorità. A riprova dell'inadeguatezza dell'attuale modello, le Linee-guida adottate dal Gruppo di lavoro sull'art. 7(f) confermano la mancanza di una visione comune sulla questione tra le autorità garanti, offrendo dettagliate spiegazioni soltanto sugli elementi della disposizione per i quali esiste già una convergenza tra i due approcci, ossia sul concetto di "interesse legittimo".³⁹ Le Linee-guida rimangono invece mute sulla seconda parte della disposizione, ovvero sui limiti entro cui i diritti fondamentali rilevanti consentono al legittimo interesse di costituire un valido fondamento di legittimità del trattamento in questo ambito. Esse forniscono una guida di carattere meramente casistico ed esemplificativo sui casi in cui un singolo trattamento può essere fondato su di un interesse legittimo, ma non risolvono la questione relativa allo *status* primario o meno del consenso nell'ambito dei diritti fondamentali così richiamati.

L'assenza di un simile coordinamento ha lasciato campo libero alle profonde differenze esistenti in dottrina e tra le tradizioni giuridiche costituzionali,⁴⁰ che sono dunque emerse, frammentando e isolando prassi e giurisprudenza nazionali.

Nella maggioranza degli ordinamenti costituzionali,⁴¹ dove il diritto alla *privacy* informazionale e/o alla protezione dei dati si fonda su un solido riconoscimento nell'ambito dell'ordinamento costituzionale, il richiamo effettuato dall'art. 7(f) ai diritti fondamentali viene inteso come volto a tutelare il diritto all'autodeterminazione dell'interessato con riguardo al trattamento dei propri dati. Il consenso rappresenta la base giuridica principale e le fattispecie alternative allo stesso sono ricostruite in maniera restrittiva, dal momento che un trattamento di dati effettuato in assenza di consenso costituisce un'interferenza con i diritti fondamentali. In tale ipotesi, un legittimo interesse di rango *sub*-costituzionale non è di per sé idoneo a legittimare un trattamento in assenza, o contro, il consenso dell'interessato; si rendono necessarie misure di legge o provvedimenti delle autorità garanti che stabiliscano la liceità

³⁹ Nella prassi, viene generalmente considerato come "interesse" qualsiasi tipo di vantaggio, anche non qualificato dalla legge, che il titolare derivi dal trattamento; quanto alla legittimità di questo, essa consisterebbe semplicemente nel non essere contrario alla legge, nell'ampio senso di non-antigiuridico; Article 29 Working Party, *Opinion 06/2014*, 844/14/EN p. 24-29. Così inteso, l'interesse a sfruttare il trattamento per finalità commerciali è idoneo a costituire un interesse legittimo ai sensi dell'art. 7(f).

⁴⁰ G. G. FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer International Publishing, Bruxelles, I ed., 2014, p. 174-206. A riprova della scarsa armonizzazione tra le tradizioni costituzionali degli Stati membri, l'autrice osserva, *inter alia*, che la Corte di Giustizia non ha ricavato il diritto alla protezione dei dati personali dalle tradizioni costituzionali comuni (art. 6(3) TUE), ma esso è entrato a far parte del diritto dell'Unione soltanto con la Carta.

⁴¹ F. FERRETTI, *The Winter of Rights?*, cit., p. 855.

tà di un simile trattamento, specificandone gli estremi e attribuendo ulteriori garanzie all'interessato.⁴² Ciò spiega, ad esempio, l'adozione di questo approccio da parte dell'ordinamento giuridico tedesco, nel quale il diritto dell'individuo a poter determinare l'eventualità che i propri dati possano essere oggetto di trattamento trova un risalente riconoscimento a livello costituzionale nelle forme del "diritto all'autodeterminazione informativa".⁴³

All'estremo opposto, nel Regno Unito la *Supreme Court* (Corte Suprema) non ha finora riconosciuto alla *privacy* lo *status* di interesse costituzionalmente protetto, nemmeno nella sua veste meramente negativa di *right to be let alone*. Di conseguenza, all'interno dell'ordinamento giuridico inglese, non esiste alcun diritto fondamentale alla *privacy* o alla protezione dei dati, al di là della limitata tutela apprestata con il recepimento dell'articolo 8 CEDU tramite lo *Human Rights Act* del 1998.⁴⁴ Questa circostanza spiega la mancata attribuzione di un ruolo prevalente al consenso rispetto alle altre basi giuridiche nell'ambito del diritto vivente inglese, come visto sopra.

⁴² F. FERRETTI, *The Winter of Rights?*, cit., p. 862-868; G. HORNUNG, C. SCHNABEL, *Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination*, in *Computer Law & Security Report*, 2009, p. 84 ss.

⁴³ Nel 1983, con la nota "sentenza sul censimento" ("*Volkszählungsurteil*" Sent. n. 1 BvR 209/834, 15 dic. 1983, 65 BVERFGE 1) la *Bundesverfassungsgericht* (Corte costituzionale federale) ha infatti ricavato un *recht auf informationelle Selbstbestimmung* ("diritto all'auto-determinazione informativa") dal più generale diritto allo sviluppo della personalità, a sua volta derivato dagli artt. 1(1) e 2(1) della legge fondamentale tedesca, i quali riconoscono, rispettivamente, il diritto alla dignità ed il diritto alla libertà personale (G. HORNUNG, C. SCHNABEL, *The Right to Informational Self-Determination*, cit., p. 84 ss.). Invero, questo diritto fondamentale si configura come assai differente dal più noto diritto alla *privacy* quale meramente negativo *right to be let alone*, così come sviluppato per la prima volta da Warren e Brandeis nel loro celebre articolo del 1890 (S. D. WARREN, L. D. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, 1890, p. 193 ss.) Sebbene questi due diritti siano in parte sovrapponibili e proteggano simili valori, tra gli elementi costitutivi del primo vi è l'attribuzione della facoltà, per l'individuo, di controllare l'utilizzo che viene fatto delle proprie informazioni personali, il quale comprende a sua volta il potere di determinare l'eventualità che questi vengano raccolti ed ulteriormente trattati o meno. Di conseguenza, ogni ipotesi in cui l'individuo non abbia avuto la possibilità di acconsentire o meno al trattamento dei propri dati costituisce un'interferenza con il presente diritto, che la Corte costituzionale tedesca ritiene accettabile solamente ove sia limitata al minimo indispensabile, sia basata su una disposizione legislativa che abbia elevati standard di chiarezza e precisione ed infine volta a perseguire altri interessi costituzionalmente protetti (G. HORNUNG, C. SCHNABEL, *The Right to Informational Self-Determination*, cit., p. 86-88). Per un'espressa adesione del Garante italiano a questa ricostruzione, si veda *ex multis* il provvedimento del 28 maggio 1997, doc. web n. 40425, dove il Garante ha stabilito che il consenso è libero se si "presenta quale manifestazione del diritto all'auto-determinazione informativa dell'interessato."

⁴⁴ F. FERRETTI, *The Winter of Rights?*, cit., p. 855; R. WACKS, *Privacy: A Very Short Introduction*, Oxford University Press, Oxford, II. ed., p. 67-61.

In ultima istanza, il diritto vivente appare decisamente influenzato dal ruolo del consenso al trattamento dei dati all'interno degli ordinamenti costituzionali nazionali.⁴⁵

Questa situazione non appare tuttavia compatibile con il diritto dell'Unione. La Corte di giustizia ha infatti stabilito che il compito delle autorità è quello di "assicurare un giusto equilibrio fra, da un lato, il rispetto del diritto fondamentale alla vita privata e, dall'altro, gli interessi che impongono una libera circolazione dei dati personali"⁴⁶ e, come si è visto nel precedente paragrafo, l'interpretazione dell'art. 7(f) e il rapporto tra questo e il consenso rappresentano un aspetto primario di questo equilibrio.

In uno scenario dove, a causa della diffusione di Internet, un gran numero di trattamenti di dati ha natura sempre più transnazionale, l'equilibrio tra tutela dei diritti e buon funzionamento del mercato interno non può essere raggiunto se ciascuna autorità attinge al diritto nazionale per risolvere la questione del rapporto tra consenso e legittimo interesse. Un simile approccio conduce necessariamente alla frammentazione del diritto vivente, creando situazioni di grave incertezza per gli operatori economici e comportando la creazione di ostacoli al libero flusso di dati e dunque al buon funzionamento del mercato interno.⁴⁷

4. L'assenza di un orientamento interpretativo consolidato nella giurisprudenza della Corte di giustizia

Negli ultimi anni, la giurisprudenza della Corte di giustizia in materia di tutela dei dati personali ha conosciuto un significativo aumento.⁴⁸ In tre occasioni, la Corte ha avuto la possibilità di esprimersi sul rapporto tra consenso e legittimo interesse. In nessun caso la questione è stata affrontata frontalmente, ma le relative sentenze forniscono alcune indicazioni relative all'atteggiamento della Corte.

La prima pronuncia è la sentenza *ASNEF*,⁴⁹ in cui la domanda pregiudiziale del giudice spagnolo verteva sulla compatibilità con l'art. 7(f) di una disposizione di legge nazionale che subordinava l'utilizzo della base dell'interesse legittimo all'ulteriore requisito che i dati personali oggetto di trattamento ri-

⁴⁵ P. BALBONI, *Legitimate interest of the data controller*, cit., p. 249-253; F. FERRETTI, *The Winter of Rights?*, cit., p. 855-858.

⁴⁶ Corte di Giustizia, sent. 6 ottobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, Causa C-362/14, ECLI:EU:C:2015:650, par. 42. In tal modo, anche nel settore dell'*enforcement* viene dunque riflessa la dualità di scopi alla base della Direttiva.

⁴⁷ P. BALBONI, *Legitimate interest of the data controller*, cit., p. 252-253.

⁴⁸ O. LYNSKEY, *The Foundations*, cit.

⁴⁹ Corte di Giustizia, sent. 24 novembre 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, cause riunite C-468/10 e C-469/10, ECLI:EU:C:2011:777.

sultassero da fonti pubbliche. Di conseguenza, nei casi di gran lunga preponderanti ove i dati personali non risultavano da fonti pubbliche, il trattamento poteva avvenire solo previo ottenimento del consenso da parte dell'interessato. La disposizione in questione sposava quindi l'idea della protezione dei dati quale diritto di autodeterminare l'utilizzo delle proprie informazioni personali.⁵⁰

La Corte ha ritenuto che la Direttiva osta alla disposizione di legge spagnola, dal momento che questa si pone in contrasto con l'obiettivo di conseguire un equilibrio tra i due valori alla base della Direttiva, ovvero la tutela della vita privata e la libera circolazione dei dati personali.⁵¹ Stabilendo che quest'ultimo valore viene in gioco nel caso di specie, la Corte ha dunque riconosciuto che l'art. 7(f) ha il proprio fondamento nella finalità di carattere mercantile, tuttavia essa non ha preso posizione sul rapporto tra legittimo interesse e consenso. I giudici dell'Unione hanno osservato che il rispetto dell'equilibrio tra questi due valori richiede che la valutazione tra legittimo interesse del titolare e diritti fondamentali dell'interessato richiesta dall'art. 7(f) venga condotta caso per caso piuttosto che effettuata *a priori* dalla legge.⁵² L'esclusione a monte di alcune categorie di trattamento basati sul legittimo interesse si configurava in contrasto con tale approccio casistico.

È vero che l'intervento del legislatore spagnolo aveva come obiettivo l'attribuzione di un ruolo di primato al consenso, e dunque di maggiore tutela ai diritti fondamentali all'interessato, ma la Corte non critica in alcun modo lo scopo alla base della disposizione di legge in esame. Piuttosto, la pronuncia è verosimilmente dettata dalla preoccupazione di evitare che ciascun legislatore nazionale, aggiungendo per legge ulteriori requisiti volti a circoscrivere l'ambito applicativo dell'art. 7(f), possa contribuire a frammentare il quadro giuridico. Questo approccio è in linea con la sentenza *Melloni*, ove la Corte ha ritenuto illegittimo il rafforzamento da parte degli Stati del livello di tutela in ambiti, come quello in esame, in cui il diritto dell'Unione ha armonizzato in maniera esaustiva le legislazioni nazionali in settori attinenti ai diritti fondamentali.⁵³ È dunque verosimile che la Corte abbia voluto evitare di porsi in contrasto con le tradizioni costituzionali nazionali di quegli Stati che, come in Spagna, riservano un ruolo primario al consenso dell'interessato, astenendosi dal prendere una posizione in merito e cercando, allo stesso tempo, di colpire la frammentazione prodotta dal differente recepimento della base giuridica.

⁵⁰ P. DE HERT, *Data Protection's Future without Democratic Bright Line Rules. Co-existing with Technologies in Europe after Breyer*, in *European Data Protection Law Review*, 2017, p. 20 ss., 28-29.

⁵¹ ASNEF, cit., parr. 34, 48 e 49.

⁵² *Ibid.*, parr. 34, 47 e 48.

⁵³ Corte di Giustizia, sent. 26 febbraio 2013, *Stefano Melloni. c. Ministero Fiscal*, causa C-399/11, ECLI:EU:C:2013:107, parr. 55-64.

Questo orientamento è stato più di recente confermato nella sentenza *Breyer*.⁵⁴ L'oggetto del rinvio pregiudiziale ricorda da vicino la questione alla base di *ASNEF*. Il giudice tedesco interrogava la Corte circa l'ammissibilità di una disposizione di legge federale che obbligava i gestori di siti *web* a raccogliere e conservare i dati personali degli utenti, in assenza di consenso degli stessi, al solo ed esclusivo fine di permettere e fatturare l'effettiva fruizione del sito da parte dell'utente. La disposizione di legge effettuava quindi essa stessa e in astratto la valutazione richiesta dall'art. 7(f) sui limiti di ammissibilità del legittimo interesse quale fondamento di liceità, fissandoli nel perseguimento di un'unica finalità ed escludendo, nel caso di specie, la possibilità per il titolare di conservare i dati degli utenti per scopi di sicurezza informatica e di perseguimento di eventuali reati commessi contro il sito.

La Corte ha reiterato quanto affermato in *ASNEF*: la normativa di uno Stato non può precludere, in astratto e categoricamente, l'effettuazione della valutazione richiesta dall'art. 7(f), dovendo invece sempre avvenire con riguardo alle circostanze concrete del caso.⁵⁵ In altre parole, è stata confermata sia la natura casistica della valutazione *ex art. 7(f)*, sia la contrarietà con il diritto dell'Unione di una misura nazionale volta a restringere il potenziale ambito applicativo della disposizione.

In *ASNEF* e *Breyer*, pur senza evocare direttamente diritti fondamentali, la Corte ha espresso una preferenza per un approccio che va nella direzione di liberalizzare la base giuridica sul legittimo interesse, escludendo la compatibilità con il diritto dell'Unione di interventi del legislatore nazionale volti a restringerne l'ambito applicativo in favore del consenso. Per tale motivo questo orientamento è stato oggetto di forti critiche da quella parte della dottrina ritiene che la possibilità, per l'individuo, di vietare ad un terzo il trattamento dei propri dati personali sia un elemento protetto dai diritti fondamentali rilevanti.⁵⁶ A questo ordine di critiche se ne può aggiungere uno ulteriore; co-

⁵⁴ Corte di Giustizia, sent. 19 ottobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland*, causa C-582/14, ECLI:EU:C:2016:779.

⁵⁵ *Breyer*, cit., par. 62.

⁵⁶ P. DE HERT, *Co-existing with Technologies in Europe after Breyer*, cit. Questo approccio diretto a rimuovere limiti fissati per legge all'ambito applicativo della disposizione, ha pesanti ripercussioni in un ordinamento giuridico, quale quello tedesco, dove il diritto all'auto-determinazione informativa gode di un saldo riconoscimento costituzionale. Infatti, altre disposizioni di legge, in questo paese, sono dirette a sancire in via generale la prevalenza del consenso sull'interesse legittimo, ponendosi dunque in esplicito contrasto con la giurisprudenza della Corte. Un esempio è rappresentato dalla disciplina sulla profilazione *online*, che stabilisce uno tra i regimi più stretti vigenti in tutta l'Unione: la profilazione è infatti lecita, ai sensi dell'art. 15(3) della legge tedesca sui tele-media, solo previo consenso, oppure qualora i dati vengano anonimizzati oppure pseudonimizzati, ma in quest'ultimo caso soggetti ad ulteriori requisiti. F. NIEMANN, L. SCHLUSSLER, *CJEU decision on dynamic IP addresses touches fundamental DP law questions*, in

me si è visto, infatti, la mancanza di omogeneità in questo ambito è soprattutto dovuta alla prassi e all'attività regolatoria dei garanti nazionali piuttosto che a misure di legge. Astenendosi dal prendere posizione sul rapporto tra consenso e legittimo interesse alla luce dei diritti fondamentali, e dunque senza elaborare criteri orientativi capaci di armonizzare il diritto vivente, la Corte lascia di fatto aperta la possibilità che i garanti e i giudici nazionali continuino a interpretare la base giuridica attingendo ai principi del rispettivo ordinamento costituzionale nazionale.

Da ultimo, la Corte di Giustizia si è pronunciata sul legittimo interesse nella sentenza *Rīgas*,⁵⁷ che si distingue dalle due sentenze appena esaminate in considerazione dell'oggetto del rinvio pregiudiziale. Quest'ultimo non verteva infatti sulla compatibilità di una normativa nazionale volta a aggiungere ulteriori elementi costitutivi alla fattispecie di cui all'art. 7(f) della Direttiva, ma sulla configurabilità, sulla base di esso, di un obbligo in capo al titolare del trattamento di comunicare i dati a un terzo, titolare di un legittimo interesse a venire a conoscenza delle informazioni personali. Nel caso di specie, in particolare, l'interesse del terzo era costituito dalla possibilità, per una società di trasporti, di conoscere le generalità di un soggetto che si era reso responsabile, in modo involontario, del danneggiamento di uno dei mezzi di trasporto della società, al fine di promuovere un'azione finalizzata a ottenere il risarcimento dei danni subiti. Nel caso di specie, la valutazione richiesta dall'art. 7(f) aveva, dunque, a oggetto l'interesse ad agire in sede civile per ottenere il risarcimento del danno, ossia un interesse senz'altro legittimo, ma non protetto da alcun diritto fondamentale. Perciò, diversamente dalla più celebre, ma meno rilevante ai fini del presente contributo, sentenza *Google Spain*,⁵⁸ dove l'interesse legittimo a trattare i dati era costituito da interessi di rango costituzionale alla libertà di espressione e di informazione, in *Rīgas* la Corte ha avuto modo di esaminare una questione in cui un interesse legittimo di rango *sub*-costituzionale costituisce l'elemento fondante del trattamento in assenza di consenso.⁵⁹

<https://www.twobirds.com/en/news/articles/2016/global/cjeu-decision-on-dynamic-ip-addresses-touches-fundamental-dp-law-questions>, 21 ottobre 2016, ultimo accesso il 20.10.2017.

⁵⁷ Corte di Giustizia, sent. 4 maggio 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde c. Rīgas pašvaldības SIA 'Rīgas satiksme'*, causa C-13/16, ECLI:EU:C:2017:43.

⁵⁸ Corte di Giustizia, sent. 13 maggio 2014, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, causa C-131/12, ECLI:EU:C:2014:317.

⁵⁹ In definitiva, mentre in *Google Spain* nell'ambito della valutazione *ex art. 7(f)* la Corte effettua un bilanciamento tra diversi diritti fondamentali (protezione dei dati e tutela della vita privata da una parte e diritto alla libertà di espressione e informazione dall'altra), in *Rīgas* l'eventuale risposta positiva della Corte al quesito posto dal giudice lettone avrebbe indicato l'accoglimento dell'approccio meno protettivo nei confronti dei diritti fondamentali.

Anche in questo caso la questione non è stata affrontata direttamente, ma la sentenza offre comunque alcuni spunti di riflessione. La Corte ha risposto al quesito in modo negativo, precisando che il testo dell'art. 7 della Direttiva è chiaro nel non porre alcun obbligo di trattare i dati.⁶⁰ In aggiunta al dato letterale, la Corte ha svolto anche un argomento sistematico, evidenziando che la Direttiva disegna una struttura generalmente proibitiva del trattamento, in considerazione del fatto che questa persegue (anche) la finalità di tutela di diritti fondamentali.⁶¹ Da ciò deriva che le basi giuridiche alternative al consenso rivestono carattere eccezionale e devono pertanto essere interpretate in modo restrittivo. Questa affermazione segna perciò un punto a favore dell'obiettivo relativo alla tutela dei diritti su quello mercantilistico, che spinge invece per una lettura più ampia possibile delle basi giuridiche *ex art. 7*.

Pur non potendosi trarre conclusioni da queste poche pronunce, l'orientamento espresso in *Rīgas* rafforza l'ipotesi – già avanzata – che l'atteggiamento della Corte in *ASNEF* e *Breyer* non miri tanto a promuovere un ampio impiego del legittimo interesse quale fondamento di liceità del trattamento a scapito del consenso, quanto sia rivolto a evitare che il legislatore di ciascuno Stato membro restringa l'ambito applicativo della base giuridica, frammentando ulteriormente il quadro giuridico. Tuttavia, non fornendo criteri e principi valutativi capaci di indirizzare in via generale l'orientamento vigente nelle prassi applicative nazionali, l'approccio casistico della Corte non appare idoneo ad arginare la tendenza alla frammentazione in atto.

5. Il rapporto tra consenso e legittimo interesse alla luce degli articoli 16 TFUE e 7 e 8 della Carta

Come si è visto nel terzo paragrafo, l'art. 7(f) è oggetto di interpretazioni contrastanti nella parte in cui dispone che un interesse legittimo possa costituire un valido fondamento di liceità soltanto “a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata”. Nell'ambito del diritto dell'Unione, i diritti e le libertà fondamentali che presidiano la normativa di protezione dei dati sono il diritto al rispetto della vita privata, protetto dall'art. 7 della Carta e dalle tradizioni costituzionali comuni degli Stati membri,⁶² e il diritto al rispetto dei dati di carattere personale, riconosciuto dall'art. 8 della Carta e dall'art. 16 TFUE.

⁶⁰ *Rīgas*, cit., par. 26.

⁶¹ *Ibid.*, par. 26, richiamandosi ai paragrafi 43-46 delle Conclusioni dell'Avvocato Generale Bobek. Questa affermazione rappresenta un importante riconoscimento, considerato che l'impronta generalmente proibitiva del trattamento non è del tutto pacifica in dottrina. O. LYNKEY, *The Foundations*, cit., p. 30.

⁶² Corte di giustizia, sent. 11 luglio 1980, *Jean Kohll contro Commissione delle Comunità europee*, causa 36/75, ECLI:EU:C:1980:200.

Come precisato dalla Corte in *ASNEF*,⁶³ la Direttiva appresta un livello di armonizzazione completo e non ulteriormente rafforzabile dagli Stati; di conseguenza, il rinvio effettuato dall'art. 7(f) ai diritti fondamentali si esaurisce all'interno dell'ordinamento giuridico dell'Unione e il limite all'utilizzabilità del legittimo interesse deve essere ricavato unicamente dai due diritti fondamentali appena citati. Pertanto, non risulta in linea con l'art. 7(f) la prassi di quelle autorità di controllo che interpretano la disposizione in esame alla luce della protezione apprestata ai diritti fondamentali dell'ordinamento giuridico nazionale.

Occorre pertanto esaminare dal punto di vista degli artt. 7 ed 8 della Carta la domanda implicitamente posta dall'art. 7(f), ossia: può un interesse, di carattere legittimo ma non altrimenti protetto dalla legge costituire un valido fondamento di liceità del trattamento in assenza del (o contro il)⁶⁴ consenso della persona interessata?⁶⁵ In altri termini, si deve stabilire se l'autodeterminazione dell'interessato in ordine al trattamento dei propri dati è un valore protetto dagli artt. 7 e 8 della Carta.

In dottrina esistono due teorie in ordine alla questione in esame,⁶⁶ che a ben vedere forniscono un sostrato teorico ai due approcci vigenti nella prassi.

Secondo una parte della dottrina, gli artt. 7 ed 8 della Carta riconoscono all'individuo un livello di controllo in linea di principio assoluto, una sorta di *habeas data*, che ricomprende il diritto di autodeterminare l'eventualità che i propri dati siano oggetto di trattamento.⁶⁷ In questa ipotesi, un trattamento di dati personali in assenza di consenso costituisce un'interferenza con i diritti fondamentali dell'individuo, con la conseguenza che un interesse legittimo di rango *sub*-costituzionale potrebbe fondare la liceità di un trattamento di dati personali soltanto ove fossero rispettate le garanzie previste dall'art. 52 della Carta.⁶⁸ Questa ricostruzione, che riconosce un ruolo primario al consenso, costituisce il fondamento teorico della prassi che considera l'art. 7(f) una base

⁶³ *ASNEF*, cit., par. 29.

⁶⁴ Come disposto dall'art. 14(a), la manifestazione di volontà contraria nel caso di trattamenti effettuati in base all'art. 7(f) può far cessare il trattamento soltanto ove l'interessato adduca "motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano," mentre l'opposizione può sempre avvenire qualora il trattamento abbia luogo "a fini di invio di materiale pubblicitario" (la disposizione viene reiterata anche nel Regolamento: *cfr. infra*, par. 6).

⁶⁵ F. FERRETTI, *The Winter of Rights?*, cit., p. 868.

⁶⁶ Ben riassunte da H. HIJMANS, *The EU as a constitutional guardian*, cit., p. 58-66.

⁶⁷ *Ex multis*: F. FERRETTI, *The Winter of Rights?*, cit., e N. PURTOVA, *Default entitlements in personal data*, cit. Questa teoria ricalca la ricostruzione operata dalla Corte costituzionale tedesca (v. nota 43).

⁶⁸ Le altre quattro ipotesi previste dall'art. 7 quali alternative al consenso, pur dovendo essere oggetto di interpretazione restrittiva, rispetterebbero il disposto dell'art. 52 della Carta, dal momento che le fattispecie da questi descritte sono previste e tipizzate dalla legge, perseguono scopi leciti in maniera proporzionata e non incidono sul contenuto essenziale dei diritti fondamentali.

giuridica dal carattere eccezionale, il cui ambito applicativo viene quindi limitato in favore del consenso della persona interessata.

Altra parte della dottrina, aderendo a una concezione procedurale della protezione dei dati personali, non ritiene che gli artt. 7 ed 8 della Carta dispongano, *prima facie*, un generale divieto del trattamento in mancanza di una decisione affermativa dell'interessato.⁶⁹ Sul piano testuale, questa teoria troverebbe riscontro nel secondo paragrafo dell'art. 8 della Carta, nella parte in cui dispone che "tali dati devono essere trattati (...) in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge".⁷⁰ Secondo tale ricostruzione, non vi è alcuna interferenza con i diritti fondamentali nel caso in cui un trattamento venga fondato su una delle basi giuridiche diverse dal consenso: ciascuna fattispecie elencata dall'art. 7 della Direttiva è ugualmente idonea a fondare la liceità di un trattamento. La protezione offerta dai diritti fondamentali si limiterebbe alle tutele ed ai diritti soggettivi attribuiti dalla normativa di protezione dei dati di diritto derivato.⁷¹ Di conseguenza, l'utilizzo del consenso o di una base giuridica alternativa allo stesso risultano del tutto indifferenti ai fini del rispetto della Carta, dal momento che l'ambito protettivo dei diritti fondamentali rilevanti si esaurisce nel riconoscere le predette garanzie di carattere procedurale e non anche nell'attribuzione della generale facoltà, per l'individuo, di determinare la possibilità che i propri dati siano oggetto di trattamento.

Ad oggi, nessuna delle due teorie sembra prevalere in dottrina né nella giurisprudenza della Corte di giustizia o delle corti nazionali. Considerata tuttavia l'impossibilità di risolvere la questione in maniera soddisfacente nell'ambito del Gruppo di Lavoro, soltanto un intervento del legislatore dell'Unione o una pronuncia della Corte potrebbero stabilire criteri comuni,

⁶⁹ H. HIJMANS, *The EU as a constitutional guardian*, cit., p. 63-66; si veda anche P. BALBONI, *Legitimate interest of the data controller*, cit.

⁷⁰ Corsivo aggiunto. Secondo la ricostruzione in esame, questo passaggio comporterebbe un'equivalenza tra il consenso e le altre cinque basi giuridiche previste dall'art. 7 della Direttiva, tra cui quella sul legittimo interesse. A tale argomentazione di carattere letterale, apparentemente inoppugnabile, altra dottrina ha tuttavia risposto rilevando che, se tale equivalenza tra consenso e legittimo interesse fosse accettata, si assisterebbe ad un'irrimediabile inconsistenza logica tra gli artt. 8(2) Carta e 7(f) della Direttiva: quest'ultimo, come già osservato, rimanda infatti a sua volta ai diritti fondamentali quali limiti alla possibilità di avvalersi del legittimo interesse, e dunque all'art. 8 della Carta, il quale tuttavia rimanda nuovamente, nel passaggio sopra riportato, non solo al consenso ma anche a qualsiasi "altro fondamento legittimo previsto dalla legge", e dunque anche all'art. 7(f), producendo così un richiamo infinito tra le due disposizioni (N. PURTOVA, *Default entitlements in personal data*, cit. p. 10-11). Di conseguenza, se interpretato quale diritto meramente procedurale, l'art. 8 della Carta non avrebbe quella forza normativa necessaria a limitare l'applicazione della disposizione sul legittimo interesse, che dunque sarebbe dotata di un ambito applicativo virtualmente illimitato.

⁷¹ Ad es. i principi relativi al trattamento dei dati, le misure di sicurezza, la supervisione da parte di un'autorità indipendente, il diritto di accesso, di rettifica, di obiezione, etc.

idonei a guidare l'opera interpretativa delle autorità di controllo e dei giudici nazionali. Una svolta in questa direzione troverebbe sponda nella speciale competenza attribuita all'Unione in materia di tutela dei dati personali. Infatti, mentre la protezione dei diritti fondamentali costituisce, in linea generale, una competenza "negativa" dell'Unione, su cui grava l'obbligo di rispettarli nell'esercizio di tutte le competenze "positive" attribuite,⁷² l'art. 16 TFUE prevede espressamente la possibilità per il Parlamento europeo e il Consiglio di adottare, mediante procedura legislativa ordinaria, "le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale" sia da parte dell'Unione sia degli Stati membri (quando attuano il diritto dell'Unione). Come è stato osservato in dottrina,⁷³ gli Stati membri hanno in tal modo attribuito all'Unione il potere di specificare, limitatamente all'ambito delineato, il livello di tutela dei diritti fondamentali ora garantiti dagli artt. 7 ed 8 della Carta.⁷⁴ Più precisamente, il legislatore dell'Unione dispone di una base giuridica specifica per un'azione nel senso indicato e, al contempo, la Corte di giustizia può contare di un margine di intervento più ampio rispetto ai diritti fondamentali oggetto di una competenza solo negativa; margine che può essere sfruttato per avanzare una compiuta concezione teorica dei diritti fondamentali alla *privacy* e alla protezione dei dati nell'ambito del diritto primario.

Un'evoluzione di tipo giurisprudenziale o legislativo nella direzione indicata non sarebbe scevra di difficoltà. L'adozione della concezione procedurale segnerebbe il riconoscimento, nell'ambito del diritto dell'Unione, di un livello di tutela più basso nei confronti dell'interessato rispetto a quello vigente nelle costituzioni degli Stati membri in cui trova protezione il diritto all'autodeterminazione dell'interessato; in altri termini, una situazione assimilabile a quella che ha dato luogo alla nota sentenza *Melloni*.⁷⁵ D'altro canto, la ricostruzione sostanziale è meno aderente all'obiettivo di carattere mercantilitico al quale comunque l'art. 16 TFUE riconosce la medesima dignità di quello relativo alla tutela dei diritti; sarebbe infatti più gravoso, se non a volte

⁷² Come riconosciuto dalla Corte al par. 27 dell'Opinione 2/94 (ECLI:EU:C:1996:140) sull'adesione della Comunità europea alla CEDU e indirettamente dagli artt. 51(2) della Carta e 6(1) TUE.

⁷³ *Ex multis*: H. HIJMANS, *The EU as a constitutional guardian*, cit.

⁷⁴ Mentre il diritto alla protezione dei dati personali è pacificamente richiamato dall'art. 16 TFUE, anche quello al rispetto della vita privata rientra nell'ambito applicativo di questo articolo, dal momento che i due diritti fondamentali hanno un ampio spazio di sovrapposizione nel loro campo applicativo, e spesso sono citati insieme nella giurisprudenza della Corte di Giustizia (*ex multis*: J. KOKOTT E C. SOBOTTA, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law*, 2013, p. 222 ss.).

⁷⁵ Corte di Giustizia, sent. 26 febbraio 2013, *Stefano Melloni. c. Ministero Fiscal*, causa C-399/11, ECLI:EU:C:2013:107.

addirittura impossibile, ottenere in via generale il consenso dell'interessato per quei trattamenti di dati che sono alla base dell'economia digitale⁷⁶ e al centro della strategia di creazione di un mercato unico digitale.⁷⁷

Ciononostante, e atteso che l'attuale stato della prassi indica una situazione in cui nessuno dei due obiettivi dell'art. 16 TFUE può dirsi pienamente realizzato, rimane auspicabile un intervento di definizione del rapporto tra consenso e legittimo interesse. Alla luce delle divergenze di ordine costituzionale identificate, sarebbe forse più opportuno preferire la via legislativa a quella dell'"imposizione" dello *standard* da parte della Corte di giustizia; vi sarebbe, così, la possibilità di comporre *ex ante* sia le divergenze tra gli ordinamenti interni, sia le tensioni tra diritto nazionale e dell'Unione che si avrebbero nel caso in cui la Corte adottasse un approccio ostile alla ricostruzione sostanziale dei diritti alla *privacy* e alla protezione dei dati personali, come potrebbe far presagire l'orientamento manifestato dalla Corte – pur non senza ambiguità – nelle pronunce esistenti relative all'art. 7(f).

6. Il potenziale impatto del Regolamento (UE) 2016/679 nel rapporto tra legittimo interesse e consenso

In attesa di una svolta nel senso auspicato, a livello legislativo o giurisprudenziale, ci si può chiedere quale ruolo potrà giocare il Regolamento (UE) 2016/679 (applicabile dal 25 maggio 2018, di seguito il "Regolamento") sul rapporto tra consenso e legittimo interesse.

La disposizione sul legittimo interesse è riproposta alla lettera (f) dell'art. 6 del Regolamento, il quale continua ad elencare anche gli altri cinque fondamenti di liceità già previsti all'art. 7 della Direttiva. A fronte di alcuni cambiamenti nella formulazione, la struttura della disposizione resta invariata, continuando a richiedere una valutazione circa i limiti entro cui i diritti fondamentali dell'individuo permettono che un trattamento possa avvenire anche in assenza del consenso di quest'ultimo.⁷⁸ La novità di maggior rilievo e impatto (soprattutto pratico) è l'inclusione delle violazioni inerenti i fondamenti di liceità del nella fattispecie sanzionatoria di maggiore gravità, con

⁷⁶ Cfr. *supra*, note 17 e 18.

⁷⁷ COM(2015) 0192 final, Bruxelles, 6.5.2015, "Strategia per il mercato unico digitale in Europa," in particolare *cf.* par. 4.1.

⁷⁸ L'art. 6(f) dispone che un trattamento di dati è lecito quando "è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore." I cambiamenti riguardano l'esplicito inserimento della necessità di prendere in considerazione la minore età del soggetto interessato nell'ambito della valutazione di liceità del legittimo interesse, mentre il successivo comma esclude la validità del trattamento fondato su questa base giuridica da parte di autorità pubbliche nell'esecuzione dei loro compiti.

sanzioni che possono raggiungere i venti milioni di euro o il 4% del fatturato mondiale annuo di un'impresa o gruppo di imprese.⁷⁹ Evidentemente, per ragioni di certezza di applicazione della sanzione, questa novità rende ancora più auspicabile e pressante una posizione uniforme con riguardo ai confini applicativi della base giuridica del legittimo interesse.

Invero, dal punto di vista strutturale, i cambiamenti più rilevanti riguardano l'altro elemento che disegna l'ambito applicativo del legittimo interesse quale fondamento di liceità, ovvero il consenso della persona interessata. La fattispecie, arricchita di nuovi elementi costitutivi, è adesso prevista all'articolo 6(a) e ulteriormente disciplinata all'articolo 7, con ben quattro paragrafi che ne stabiliscono in dettaglio i requisiti.⁸⁰

Il Regolamento adotta dunque un approccio più rigoroso rispetto alla Direttiva: mentre quest'ultima lasciava spazio a consensi solo apparenti, nel Regolamento il legislatore dell'Unione ha disciplinato la fattispecie in modo da attribuire agli individui la possibilità di esprimere una scelta realmente libera e informata.⁸¹ Si tratta di modifiche dirette a valorizzare il diritto dell'individuo ad autodeterminare l'eventualità che un terzo possa procedere al trattamento dei propri dati e che in apparenza segnalano un'adesione all'idea del consenso dell'interessato al trattamento come un valore tutelato dagli artt. 7 ed 8 della Carta.

Tuttavia, allargando lo sguardo alla generale struttura del Regolamento, le modifiche appena considerate potrebbero comportare, paradossalmente, un'ulteriore perdita di centralità del consenso quale fondamento di legittimità del trattamento.⁸² A ben vedere, infatti, non è prevista alcuna indicazione circa l'esistenza di una gerarchia tra le basi giuridiche e non viene specificato quale sia il punto di equilibrio tra necessità di richiedere il consenso dell'interessato e possibilità di avvalersi del legittimo interesse. In altri termini, il Regolamento non richiede, di per sé, di privilegiare il previo assenso dell'interessato al fine di legittimare un trattamento di dati, lasciando anzi del

⁷⁹ Art. 83(5) del Regolamento.

⁸⁰ Per essere valido, esso non può essere generico ma deve riguardare "una o più specifiche finalità" (Art. 6(a)), deve essere presentato "in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro" (Art. 7(2)) e non può essere richiesto nei casi in cui la mancata prestazione dello stesso comporti conseguenze pregiudizievoli per l'interessato, compresa la mancata esecuzione di un contratto o prestazione di un servizio (Art. 7(4), considerando 42 e 43). Infine, esso non sarà generalmente considerato valido nei casi in cui vi sia un considerevole squilibrio di potere tra l'interessato e il titolare del trattamento, ad esempio nel caso di rapporti tra privati e autorità pubbliche (considerando 43), ovvero nel caso in cui l'interessato sia un minore di sedici anni (art. 8). L'onere di dimostrare che il consenso presenta tutti i requisiti richiesti grava infine in capo al titolare (Artt. 7(1) e 24(1)).

⁸¹ Considerando 32 e 33.

⁸² *Ex multis*: P. BALBONI, *Legitimate interest of the data controller*, cit.; N. PURTOVA, *Default entitlements in personal data*, cit..

tutto aperta la possibilità di interpretare queste due basi giuridiche come dotate della medesima importanza. Ancora una volta, la limitazione all'utilizzabilità del legittimo interesse passa per il rinvio immediato ai diritti fondamentali, richiamati dalla seconda parte della disposizione.

Dal punto di vista pratico, il Regolamento potrebbe incentivare i privati ad avvalersi dell'art. 6(f), per una serie di motivi che saranno adesso considerati. In primo luogo, come già osservato, già con i meno rigorosi requisiti richiesti dalla Direttiva buona parte dei trattamenti di maggiore interesse economico portati avanti tramite l'utilizzo di nuove tecnologie sono, di fatto, impossibili o estremamente difficili da legittimare mediante l'ottenimento di un valido consenso. Il rafforzamento dei requisiti di quest'ultimo da parte del Regolamento renderà dunque ancora più difficoltosa la legittimazione del trattamento ai sensi dell'art. 6(a). È quindi verosimile che la mancanza di un'espressa gerarchia tra il consenso e le altre basi giuridiche spingerà gli operatori economici che fanno uso di simili tecnologie a ricercare nel proprio (legittimo) interesse economico il fondamento di liceità per i trattamenti di dati eseguiti nell'ambito della propria attività commerciale.

Questa tendenza è ulteriormente rafforzata dal fatto che, in corso di trattamento, la disciplina relativa ai diritti soggettivi dell'interessato rende ancora meno conveniente per un'impresa privata avvalersi del consenso. Infatti, nel caso in cui il trattamento di dati sia fondato sull'art. 6(a), la persona interessata ha, in qualsiasi momento, senza necessità di giustificazione e senza bisogno di alcuna formalità, la possibilità di revocare il proprio consenso, facendo così venir meno la liceità del trattamento.

Al contrario, considerato in corso di trattamento, il legittimo interesse appare un fondamento di liceità decisamente più stabile. Infatti, nell'ambito di un trattamento fondato sull'art. 6(f), l'art. 21(1) dispone che la manifestazione da parte dell'interessato della volontà di interromperne l'esecuzione ne farà venir meno la liceità non in maniera incondizionata, ma soltanto "per motivi connessi alla sua situazione particolare", e, ove ricorra una tale situazione, fatta comunque salva "l'esistenza di motivi legittimi cogenti (...) che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure (...) l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria".⁸³

A ciò si aggiunge, infine, l'estensione del nuovo diritto alla portabilità dei dati previsto dall'articolo 20 del Regolamento, il quale comprenderà i trattamenti fondati sull'art. 6(a), ma non quelli fondati sull'art. 6(f). Questo nuovo diritto, che obbliga il titolare a fornire all'interessato i dati personali in "un

⁸³ Il secondo par. dell'art. 21 dispone che la volontà dell'interessato contraria ad un trattamento effettuato in base all'art. 6(f) ne farà venir meno la liceità soltanto nei casi di *marketing* diretto e profilazione.

formato strutturato, di uso comune e leggibile da dispositivo automatico” ed anche ad inviare direttamente i dati ad un altro titolare “ove tecnicamente fattibile”, si preannuncia un adempimento decisamente gravoso da soddisfare per il titolare del trattamento, sul lato sia tecnico sia organizzativo, tanto che sono state espresse preoccupazioni⁸⁴ per l’ampia interpretazione della disposizione effettuata dal Gruppo di Lavoro nelle linee-guida emanate a riguardo.⁸⁵

A tutto ciò va sommata la circostanza che, in coerenza con il principio di responsabilizzazione introdotto dal Regolamento all’art. 5(2), la scelta in ordine alla base giuridica da utilizzare è, *prima facie*, rimessa al titolare del trattamento, con un controllo in linea di principio soltanto successivo dell’autorità garante nazionale.⁸⁶ Visti i vantaggi presentati dall’art. 6(f) rispetto al 6(a), il titolare sarà verosimilmente spinto a evitare di dover ottenere il consenso dell’interessato ove possibile.

In sintesi, mentre il Regolamento, dal lato teorico, sembra rafforzare il ruolo del consenso nell’ambito della protezione dei dati, provvedendo a regolarlo in maniera più stringente rispetto alla Direttiva, sul piano pratico il principio di responsabilizzazione e le modifiche appena esaminate rischiano di espandere ulteriormente l’utilizzo della fattispecie di cui all’art. 6(f).

Allo stesso tempo, però, il Regolamento interviene in modo incisivo sull’attuale, quasi inesistente, modello di coordinamento tra le autorità, con lo scopo dichiarato di garantire “una cooperazione efficace tra le autorità di controllo dei diversi Stati membri”.⁸⁷ Con tale meccanismo il legislatore dell’Unione mostra di essere ben consapevole delle attuali problematiche di frammentazione e scarsa armonizzazione.

Innanzitutto, il legislatore dell’Unione ha rivisto in maniera capillare le regole che disciplinano la competenza delle autorità chiarendo i casi in cui, in base al principio di territorialità, essa è inderogabilmente attribuita a un’autorità in via esclusiva, inserendo altre ipotesi in cui la competenza di un’autorità si presume tale in via relativa e introducendo, infine, la nozione di trattamento transfrontaliero di dati.⁸⁸

⁸⁴ D. MEYER, *European Commission, experts uneasy over WP29 data portability interpretation* in <https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation/>, 25 aprile 2017, ultimo accesso il 20.10.2017.

⁸⁵ Article 29 Working Party, *Guidelines on the right to data portability*, 16/EN.

⁸⁶ Si tratta dunque di un approccio contrario a quello adottato dal legislatore italiano all’art. 24(g) del Codice Privacy e volto a restringere la possibilità di avvalersi del legittimo interesse (*cf. supra* par. 3).

⁸⁷ Considerando 13 del Regolamento.

⁸⁸ Definito all’art. 4(23) del Regolamento: “a) trattamento di dati personali che ha luogo nell’ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell’Unione ove il titolare del trattamento o il responsabile del tratta-

Un secondo intervento riguarda la cooperazione tra autorità nei casi di trattamento transnazionale, con la creazione del meccanismo dello “sportello unico,” che sostituisce la generica clausola di collaborazione prevista all’art. 28(6) della Direttiva. Nei casi di trattamento transfrontaliero, il Regolamento conferisce all’autorità dello Stato nel cui territorio è ubicato lo stabilimento principale del titolare lo *status* di “autorità capofila”, mentre le autorità di altri Stati membri che presentano un rilevante collegamento con il trattamento in questione assumono il ruolo di “autorità interessata”,⁸⁹ dovendo essere coinvolte nel procedimento dalla capofila. Le autorità interessate possono obiettare alla proposta di provvedimento che la capofila intende adottare alla conclusione di un’investigazione, obbligando in tal modo la capofila a riconsiderare la propria misura.

Il terzo e più importante intervento riguarda la creazione di un organismo avente personalità giudica, il “Comitato europeo per la protezione dei dati”, destinato a succedere al Gruppo di Lavoro. Pur riproducendo la composizione del predecessore, il Comitato è tuttavia dotato di poteri anche vincolanti, in due casi molto importanti: “[quando] un’autorità di controllo nazionale intenda adottare provvedimenti vincolanti riguardanti trattamenti che incidono in maniera sostanziale un numero significativo di persone interessate in più di uno Stato membro”⁹⁰ e “[quando], nell’ambito del meccanismo di cooperazione, l’autorità capofila e le autorità interessate non raggiungano un accordo sulla misura da adottare, ovvero vi sia disaccordo sulla competenza di una o più autorità”.⁹¹

In quest’ultima ipotesi, il Comitato agisce dunque come organismo di risoluzione di controversie interpretative che dovessero insorgere tra due o più autorità di controllo nazionali. Il Comitato potrebbe pertanto essere investito di una questione riguardante il rapporto tra consenso e interesse legittimo, qualora due o più autorità (in veste di autorità capofila o interessata) con orientamento opposto sull’interpretazione dell’art. 6(f) si trovassero ad avere contemporaneamente competenza in un caso di trattamento transfrontaliero.

mento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell’ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell’Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.”

⁸⁹ Vale a dire nel caso in cui il titolare o responsabile del trattamento ha uno stabilimento nel territorio dello Stato membro di appartenenza, nel caso in cui il trattamento incide in modo sostanziale sugli interessati residenti nel territorio dello Stato membro di appartenenza o, infine, nel caso in cui è stato proposto un reclamo all’autorità (art. 56 del Regolamento).

⁹⁰ Art. 64(1) del Regolamento. Il Comitato decide a maggioranza semplice in questi casi (art. 64(3)).

⁹¹ Art. 65(1) del Regolamento. A maggioranza di due terzi dei propri componenti (art. 65(2)).

A differenza del sistema attualmente applicabile, le nuove regole sulla competenza e l'istituzione del Comitato potranno favorire un confronto diretto tra le differenti prassi attualmente vigenti a livello nazionale, assoggettando la controversia ad una decisione vincolante per tutte le autorità di controllo. Peraltro, le decisioni del Comitato sono impugnabili ai sensi dell'art. 263 TFUE,⁹² circostanza che potrebbe facilitare la possibilità, per la Corte, di esprimersi sul ruolo degli artt. 7 e 8 Carta nella modulazione del rapporto tra consenso e legittimo interesse.

7. Osservazioni conclusive

La mancanza di una dimensione comune in ordine alla natura dei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta non permette il raggiungimento di un equilibrio soddisfacente tra i due obiettivi alla base della normativa dell'Unione di protezione dei dati personali.

A fronte dei potenziali problemi che deriverebbero dall'accoglimento, per via legislativa o giurisprudenziale, dell'una o dell'altra ricostruzione prevalente nelle tradizioni costituzionali nazionali, ovvero quella sostanziale e quella procedurale, il raggiungimento di una dimensione comune resta in ogni caso la soluzione più opportuna. In coerenza con la prossima applicabilità del nuovo Regolamento, che segnerà il passaggio verso un quadro giuridico uniforme, si rende infatti auspicabile un'interpretazione omogenea del rapporto tra consenso e legittimo interesse nella prassi e nella giurisprudenza nazionale degli Stati membri.

L'istituzione del "Comitato europeo per la protezione dei dati" e la creazione del nuovo meccanismo di coordinamento da parte del Regolamento rappresentano un importante viatico per raggiungere, se del caso anche in maniera conflittuale, un'omogeneità applicativa tra le prassi delle diverse autorità di controllo, evitando al contempo gli inconvenienti che deriverebbero da una netta presa di posizione da parte della Corte.

⁹² Considerando 143 del Regolamento. Nel caso in cui i ricorrenti siano persone fisiche o giuridiche, gli artt. 256 TFUE e 51 dello Statuto della Corte (*a contrario*) attribuiscono la competenza in primo grado al Tribunale, le cui decisioni saranno appellabili presso la Corte solo per questioni di diritto.