MERCATO UNICO DIGITALE, DATI PERSONALI E DIRITTI FONDAMENTALI

a cura di Francesco Rossi Dal Pozzo

UNIVERSITÀ DEGLI STUDI DI MILANO
DIPARTIMENTO DI DIRITTO PUBBLICO ITALIANO E SOVRANAZIONALE
Centro di Eccellenza Jean Monnet
Via Festa del Perdono, 7 - 20122 Milano - Italia/Italy

Co-funded by the Erasmus+ Programme of the European Union

ISSN 2384-9169

Fascicolo speciale
"*Mercato Unico Digitale, dati personali e diritti fondamentali*"
Pubblicato nel luglio 2020
http://rivista.eurojus.it

Editore: Bruno Nascimbene, Milano
Rivista registrata presso il Tribunale di Milano, n. 278 del 9 settembre 2014 Eurojus © è un marchio registrato

Il presente Fascicolo speciale, contenente gli Atti del Convegno tenutosi il 16 dicembre 2019 nella Sala Napoleonica dell'Università degli Studi di Milano, è stato pubblicato con il contributo del Centro di Eccellenza Jean Monnet *"Mercato Unico Digitale e Cybersecurity" dell'Università degli Studi di Milano diretto dal Prof. Francesco Rossi Dal Pozzo*

INDICE

Introduzione

Di MARINA AVERANI [*]

Buongiorno a tutti a nome dell'AIGE e del suo Presidente Prof. De Caterini che oggi non ha potuto essere presente. Desidero in primo luogo ringraziare il Dipartimento di Diritto Pubblico italiano e sovranazionale dell'Università degli Studi di Milano, e con particolare piacere il Direttore Professoressa Lorenza Violini per le belle parole che ci ha rivolto, oltre al Centro di Eccellenza Jean Monnet, specificatamente nella persona del Prof. Rossi Dal Pozzo per il gradito invito ad organizzare insieme questo incontro di studi.

AIGE è un'associazione che sin dagli inizi ha seguito con attenzione e passione l'evoluzione del sistema giuridico europeo.

Sono già passati 60 anni da quando un gruppo di giuristi di ogni settore, avvocati, sia dello Stato che del libero foro, magistrati e accademici (mi permetto di sottolineare questa diversità di natura perché è tuttora l'elemento peculiare AIGE), tutti pervasi da uno identico spirito di grande entusiasmo europeo, fondarono un'associazione senza scopo di lucro con l'intento di diffondere il diritto comunitario allora nascente. A quei tempi la missione dell'Aige era quasi esoterica, così come lo era il suo diritto europeo, disciplina di nicchia della quale pochissimi conoscevano l'esistenza. Non c'erano cattedre universitarie, era una materia sconosciuta alla grande massa degli avvocati e dei magistrati, le controversie di diritto comunitario erano patrimonio di pochi studi altamente specializzati.

In tutti questi anni, come previsto dal suo Statuto, grazie agli autorevoli Presidenti che si sono succeduti – e permettetemi al riguardo di rivolgere un saluto affettuoso al qui presente nostro Past Presidente Prof. Giuseppe Tesauro – ed a tutti i Soci che vi si sono dedicati volontariamente e disinteressatamente, AIGE ha promosso sia a livello nazionale che internazionale attività scientifiche (convegni, conferenze, dibattiti, seminari), attività di formazione (corsi di aggiornamento teorico/pratici, corsi istituzionali di diritto comunitario sia di base che avanzati , giornate di alta formazione) attività editoriali (pubblicazione di atti di convegni, di seminari, di studi) oltre che attività di ricerca e partecipazione a progetti comunitari, non fermandosi però soltanto alla speculazione scientifica tout-court, momento pur essenziale ma seguendo un metodo che la nostra Associazione considera utile, fattivo, addirittura necessario (forse proprio data la sua origine composita): quello dell'applicazione. senza mai abdicare all'idea originaria di collegare dogmatica e pratica.

[*] Segretario generale AIGE (Associazione Italiana Giuristi Europei).

Molte di queste iniziative sono state effettuate in collaborazione con altri interlocutori, ugualmente coinvolti nelle questioni comunitarie, dalla più varia natura: istituzionale , accademica, tecnica o formativa (Avvocatura dello Stato, AGCM, la Rappresentanza in Italia della Commissione Europea, CNF , Consigli dell'ordine di varie città, SEU, Agi, UAE, l'ANM, la Scuola Superiore della Magistratura), oltre naturalmente a molteplici Università italiane e straniere ed anzi proprio a questa prestigiosa Università, in virtù del legame con il Prof. Nascimbene, ci lega una lunga tradizione (ricordo da ultimo il ciclo di eventi "Concorrenza ed effettività della tutela tra ordinamento dell'Unione Europea e ordinamento italiano" implementazione di un progetto rientrante nel programma Jean Monnet).

Interlocutori volutamente ricercati nell'ottica del dialogo e del confronto, laddove non addirittura protagonisti empirici, come nell' ultimo format che abbiamo esperito, i pomeriggi dell'AIGE, presentando testimonianze dirette di istituzioni e di operatori che si confrontano in prima linea quotidianamente con le problematiche degli argomenti via via oggetto di discussione.

Però AIGE fu anche nel 1961 tra i fondatori della Fédération Internationale Pour Le Droit Européen (più conosciuta con l'acronimo FIDE), la più autorevole rete di associazioni nazionali che si occupano di diritto europeo, ne è tuttora l'unico rappresentante italiano ed in tale veste ha da sempre intrattenuto le relazioni con le altre consorelle, oltre ad assicurare la presenza italiana e la presentazione delle relazioni nazionali ai convegni FIDE.

Questi convegni, organizzati biennalmente nelle capitali degli stati membri a seconda dell'associazione nazionale che assicura la presidenza , hanno accompagnato l'evoluzione del diritto comunitario, seguendone costantemente lo sviluppo, intervenendo da un punto di vista scientifico ed operativo, coniugando gli aspetti dogmatici con quelli applicativi e rappresentano tuttora l'assise più importante e prestigiosa per tutti coloro che s'interessano al processo d'integrazione europea, data anche la costante fattiva partecipazione delle stesse istituzioni europee (*in primis* della Corte di Giustizia).

Si tratta di convegni dalla struttura particolare (consolidatissima, siamo giunti ormai alla ventinovesima edizione) incentrata su tre argomenti, i "cd topics", tutti su temi importanti e tecnicamente impegnativi dell'attualità europea*,* in genere uno di carattere istituzionale, uno avente ad oggetto un qualche aspetto del mercato interno e l'altro in materia di politica di concorrenza, caratterizzati da un iter di preparazione piuttosto lungo, praticamente senza discontinuità da un convegno all'altro.

Difatti dopo un accurato e dibattuto processo di selezione tra le Associazioni Nazionali dei tre argomenti che saranno oggetto del Convegno, viene individuato un relatore generale che prepara un accurato questionario sull'argomento; vengono successivamente indicati da ciascuna associazione i rispettivi relatori nazionali, che preparano le relazioni con le risposte ai singoli punti del questionario.

Vengono poi predisposti gli atti, contenenti il questionario, le relazioni nazionali, un Rapporto Generale preparato dal Rapporteur general ed integrato da un rapporto istituzionale redatto da un rappresentante delle istituzioni UE, che costituiscono la base

per la discussione delle giornate di lavoro del Convegno, che si svolgono dapprima per panels separati, a seconda dei vari topics, per riunirsi poi nella sessione conclusiva generale, riassuntiva di tutto il dibattito svoltosi.

La nostra associazione ha varato la prassi di dedicare un incontro di riflessione ad ognuno dei 3 topics, affidandone la presentazione ai relatori nazionali per suscitare poi sulle tematiche, sempre attualissime, del questionario, un dibattito tra i presenti, non solo Soci AIGE, ma anche tutti coloro che vi siano interessati, e magari incoraggiarli a partecipare al Convegno FIDE.

Orbene, tra i 3 temi prescelti per il prossimo Convegno, che si svolgerà a l'AJA dal 20 al 23 al maggio p.v., quello relativo al mercato interno è dedicato proprio alla protezione dei dati personali.

Nell'ambito di quella che ormai è definita la quarta rivoluzione industriale, la protezione dei dati personali ha acquistato sempre più importanza: con l'adozione del GDPR l'UE ha voluto fissare un alto livello di protezione, enunciando dei parametri di riferimento anche a livello mondiale, con particolare riguardo agli aspetti procedurali, di merito ed anche istituzionali che vi sono connessi, che non possono non interessare tutti i giuristi, e non solo loro.

L'intento del Convegno FIDE, come ben è emerso dal dibattitto prodromico sollecitato dalla presidenza olandese che si è poi sviluppato tra le varie associazioni nazionali per arrivare all'esatta definizione del tema , vuol essere quello di redigere un primo bilancio della nuova disciplina esattamente a due anni dalla sua entrata in vigore: dal momento che le disposizioni che la compongono lasciano un notevole margine agli Stati per legiferare, nel relativo questionario si chiede di esaminare il modo in cui sono stata integrate negli ordinamenti giuridici nazionali e quello in cui sono state risolte eventuali situazioni di conflitti di diritti, oltre a voler fare il punto sull'applicazione e sull'interpretazione datane dalla Corte di Giustizia, dalle giurisdizioni dei singoli Stati membri e dalle autorità nazionali incaricate della protezione dei dati.

Ed ecco spiegata la presenza qui oggi di AIGE: difatti la scelta del relatore nazionale su questa tematica, seguendo anche l'indicazione pervenutaci da AISDUE, è stata proprio quella di indicare il Socio Prof. Francesco Rossi Dal Pozzo, data la Sua conclamata competenza ed autorevolezza in materia.

Parlando prima dell'estate riguardo all'incontro scientifico che avevamo intenzione di organizzare riguardo a questo topic, ci prospettò l'idea di svolgerlo in concomitanza e nell'ambito di un più ampio Convegno che lui stesso stava allora cominciando a preparare.

Riscontrata quindi una perfetta sintonia di intenti, ha avuto origine e si è sviluppato un efficace connubio nel concepire e strutturare i lavori preparatori che hanno portato alla realizzazione dell'evento odierno, frutto di una continua e costante collaborazione, che ha concretizzato per esempio il nostro suggerimento di esaminare anche l'interazione con altri campi del diritto come quello amministrativo o penale, ma soprattutto ha contemplato la previsione di specifici interventi, svolti tra l'altro da relatori di altissimo livello, che affrontano alcuni dei punti chiave del questionario FIDE, come ad esempio

quale sia stata l'applicazione del GDPR a livello nazionale, quali modifiche abbia comportato sugli ordinamenti giuridici nazionali , quale sia stata l'incidenza dell'articolo 8 della Carta dei diritti fondamentali, la relativa giurisprudenza della Corte di Giustizia, lo sviluppo del mercato unico digitale, i rapporti con la politica della concorrenza.

Ma non spetta certo a me entrare nel merito delle tematiche oggetto di un così importante incontro di studio: rivolgo quindi ancora un grande plauso al Prof. Rossi Dal Pozzo per l'ottima organizzazione di questo Convegno, che si presenta con tutte le premesse per un rilevante ed eccellente successo.

Qualche considerazione d'insieme sul mercato unico dei dati e la loro tutela nell'Unione europea

DI FRANCESCO ROSSI DAL POZZO *

Questo numero speciale della Rivista *Eurojus* ospita gli atti del Convegno "Mercato Unico Digitale, tutela dei dati personali e diritti fondamentali" del 16 dicembre 2019, organizzato dal Centro di Eccellenza *Jean Monnet* dell'Università degli Studi di Milano e da AIGE, che ringrazio anche per avermi dato l'opportunità di occuparmi di questi temi in qualità di relatore nazionale per il prossimo congresso FIDE, e con il sostegno di AISDUE e ASSONIME.

Il filo conduttore dei contributi di questo numero speciale della Rivista è la ricerca di un equilibrio fra libera circolazione e protezione dei dati.

Un equilibrio che non è semplice trovare specie nel settore digitale dove tutto si muove a un ritmo accelerato: un ritmo che si impone non solo a chi opera in questo campo, ma anche a chi è chiamato a stabilire le regole e a chi è tenuto ad assicurare che tali regole non soltanto siano rispettate, ma non finiscano per confliggere con principi giuridici che vengono enunciati e riconosciuti molto più lentamente e che, anche per questo motivo, sono ad esse gerarchicamente sovraordinati.

Negli ultimi anni si è, inoltre, assistito a una crescita esponenziale in termini di quantità, qualità e diversità delle attività di trattamento dei dati che ha finito per generare una progressiva tensione fra l'esigenza di tutelare il singolo cui quei dati si riferiscono e quella di garantire la circolazione delle informazioni per finalità sociali, economiche e di pubblica sicurezza.

Di qui la difficoltà nel delimitare la disciplina sul piano concettuale e applicativo proprio in ragione della eterogeneità dei fini possibili cui si prestano i dati che, se personali, oggi rappresentano indubbiamente una componente essenziale dell'identità di ciascun individuo.

Con questa consapevolezza, l'Unione europea si è dotata di un quadro giuridico, molto eterogeneo, che poggia essenzialmente su tre pilasti: *a*) migliorare l'accesso dei consumatori e delle imprese ai beni e servizi digitali; *b*) creare un contesto favorevole affinché le reti e i servizi digitali possano svilupparsi; *c*) massimizzare il potenziale di crescita dell'economia digitale. Questo nuovo quadro giuridico trae ispirazione dal "Programma di Stoccolma — Un'Europa aperta e sicura al servizio e a tutela dei cittadini" (in *GUUE* L 115 del 4 maggio 2010, p. 1), in cui il Consiglio europeo ha invitato la Commissione a valutare il funzionamento degli strumenti giuridici dell'Unione in materia

* Professore ordinario di diritto dell'Unione europea e Direttore del Centro di Eccellenza *Jean Monnet* sul Mercato Unico Digitale dell'Università degli Studi di Milano.

di protezione dei dati e a presentare, se quest'ultima lo avesse ritenuto necessario, iniziative a carattere legislativo o anche prive di tale natura.

In una successiva comunicazione del 2010 (COM(2010) 609 def), dal titolo "Un approccio globale alla protezione dei dati personali nell'Unione europea", la Commissione ha sostenuto che l'Unione europea avesse bisogno di una politica più completa e coerente in tema di protezione dei dati personali.

La *ratio* di una tale riforma organica è da rinvenirsi nella necessità di introdurre specifiche regole in grado di rispondere alle nuove sfide che la tecnologia e il suo evolvere pongono rispetto al diritto alla tutela dei dati personali. Si avvertiva già allora, dunque, l'esigenza di adeguare l'impianto normativo al nuovo contesto tecnologico, al fine di instaurare un clima di fiducia negli ambienti on line e permettere al tempo stesso un continuo sviluppo economico, fondato su applicazioni tecniche innovative.

Di certo, oggi ci troviamo in presenza di un quadro giuridico in materia profondamente innovato, sebbene ancora incompleto, ma anche piuttosto frammentato tanto da rendere non sempre agevole il coordinamento dei vari atti che sono stati sino ad ora adottati.

Per questo motivo la realizzazione di un mercato unico digitale, completo e coerente, rappresenta per l'Unione europea ancora una sfida su cui concentrare i propri sforzi negli anni a venire, tenuto conto che si tratta di un settore vitale anche sul piano della crescita economica.

Non a caso, fra le sei priorità individuate dalla nuova Commissione (Orientamenti politici della Commissione 2019-2024 del 16 Luglio 2019) figura la creazione di un'Europa pronta per l'era digitale. A riprova, però, che l'Europa pronta non lo è ancora.

Una nuova realtà con cui anche le Corti (di giustizia e EDU) si sono dovute misurare, e lo hanno fatto con non poca fatica, proprio per la complessità e la delicatezza dei profili che entrano in gioco, spesso rappresentativi di interessi diversi, talora persino contrapposti, ma ugualmente meritevoli di tutela.

Ora, è superfluo ricordare che il nuovo impianto normativo codifica, anche in un contesto digitale, una giurisprudenza evolutiva della Corte di giustizia grazie alla quale la tutela dei dati personali ha assunto nel tempo connotazioni diverse per giungere oggi a una configurazione orientata sui diritti fondamentali.

Non è certamente possibile qui richiamare neanche per sommi capi questo lungo processo evolutivo, che potremmo definire di costituzionalizzazione del diritto alla protezione dei dati personali.

Ma come non menzionare la storica sentenza *Stauder* del 12 novembre 1969 (causa 29/69, ECLI:EU:C:1969:57) che, come è noto, rappresenta una delle prime pronunce nelle quali la Corte si è fatta carico del compito di tutelare, in un contesto di primordiale integrazione politica degli ordinamenti nazionali, i diritti fondamentali della persona, in quanto parte dei principi generali del diritto, sia pure nei limiti della loro compatibilità con la struttura e le finalità della allora Comunità economica europea. Già in questa risalente pronuncia, che anticipa l'ampia e complessa giurisprudenza della Corte sul bilanciamento fra diritti fondamentali differenti, di cui si dirà in seguito, emerge l'obbligo

per gli Stati membri di individuare, tra le possibili misure in grado di conseguire l'obiettivo prefissato, quelle meno pregiudizievoli dei diritti della persona, incluso il diritto alla riservatezza. I diritti fondamentali assurgono, dunque, a parametro di legittimità dei comportamenti degli Stati membri in attuazione del diritto comunitario e in questo quadro prende forma il diritto alla protezione dei dati personali quando il loro utilizzo si riverbera e interferisce sulla vita privata dell'individuo.

Si potrebbero poi citare le sentenze *Adams* (sentenza del 7 novembre 1975, causa 145/83, ECLI:EU:C:1985:448), *National Panasonic* (sentenza del 26 giugno 1980, causa 136/79, ECLI:EU:C:1980:169) e *AM & S* (sentenza del 18 maggio 1982, causa 155/79, ECLI:EU:C:1982:157), ma l'elenco è certamente molto più ampio e diventerà sterminato a partire dal 1996, anno di entrata in vigore della direttiva n. 95/46/CE (in *GUCE* L 281 del 23 novembre 1995, p. 31), oggi sostituita dal Regolamento (UE) n. 2016/679 (in *GUUE* L 119 del 4.5.2016, p. 1), nelle cui disposizioni la Corte ha trovato un fondamento più solido per le proprie pronunce.

Ed è proprio grazie a una giurisprudenza evolutiva che il diritto alla protezione dei dati personali è stato qualificato nel tempo come fondamentale anche nell'ordinamento dell'Unione europea.

Un diritto (fondamentale) poi divenuto, con l'art. 8 della Carta, autonomo, almeno sul piano formale perché, a dire il vero, questa autonomia tuttora fatica ad emergere anche nella giurisprudenza più recente in quanto il collegamento con la sfera privata e familiare pare configurarsi come l'elemento distintivo fra i dati personali e i dati non personali che si muovono solo in apparenza lungo binari paralleli.

Di certo, l'art. 8 della Carta dei diritti fondamentali rappresenta il punto di arrivo di un processo di codificazione e costituzionalizzazione del diritto alla protezione dei dati personali e al tempo stesso costituisce la pietra angolare del nuovo impianto normativo di cui l'Unione si è dotata.

Anche se il diritto alla protezione dei dati personali, come ricorda la Corte in diverse pronunce, non costituisce una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale, per cui, al ricorrere di determinate condizioni, esso può essere sottoposto a limitazioni, a mente dell'art. 52, paragrafo 1 della Carta.

E la Corte, interpretando le norme di diritto derivato, si è trovata sovente a operare un bilanciamento con altri diritti fondamentali.

Il capitolo più delicato è quello che vede in apparente contrapposizione il diritto alla tutela dei dati personali e l'interesse generale alla sicurezza e alla prevenzione dei reati.

La giurisprudenza della Corte di giustizia (*Digital Rights Ireland* dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238, in cui, peraltro, la Corte ha deciso per la prima volta nella storia del processo di integrazione europea di dichiarare nullo un atto di diritto derivato dell'Unione perché in contrasto con la Carta dei diritti fondamentali (articoli 7, 8 e 52, paragrafo 1), avendo il legislatore UE ecceduto i limiti imposti dal rispetto del principio di proporzionalità, *Tele 2 Sverige* del 21 dicembre 2016, causa C-203/15, ECLI:EU:C:2016:970 e *Ministerio Fiscal* del 2 ottobre 2018, causa C-207/16, ECLI:EU:C:2018:788) ci indica una strada.

Il delicato equilibrio fra limitazioni dei diritti fondamentali ed esigenze securitarie passa, pertanto, sotto il vaglio di un test di (stretta) proporzionalità che consente alla Corte di valorizzare la centralità del diritto alla protezione dei dati e del diritto al rispetto della vita privata e che, integrando il test di necessità, si pone come meccanismo di salvaguardia a difesa dei valori di una società democratica.

Certo, viene da chiedersi sino a che punto la protezione dei dati personali con la sua nuova fisionomia di diritto fondamentale possa talora prevalere non solo su interessi di carattere economico e sociale, ma anche su esigenze di sicurezza.

La risposta è problematica perché la strada per trovare un equilibrio tra queste istanze è molto scivolosa.

La protezione dei dati personali non è solo un diritto individuale, ma rappresenta anche un interesse pubblico, una garanzia per la vita democratica e, dunque, per i valori su cui si fonda l'Unione e al tempo stesso la sicurezza non è solo un bene pubblico, ma è anche un diritto individuale. Un bisogno primario dell'uomo che egli è naturalmente portato ad appagare unendosi a una comunità alla ricerca di protezione. Quella comunità è oggi l'Unione europea su cui grava un'obbligazione anche di carattere positivo.

D'altra parte, l'art. 6 della Carta ci dice che ogni persona ha diritto alla libertà e alla sicurezza, sebbene il significato di quest'ultima espressione, cui si fatica a riconoscere la dignità di diritto autonomo, sia nella giurisprudenza della Corte ancora indefinito.

Insomma, il rapporto fra protezione dei dati personali e sicurezza non va visto necessariamente in una dimensione antinomica.

Questi e molti altri temi saranno affrontati negli scritti che seguono.

L'auspicio è che questa iniziativa del Centro di Eccellenza *Jean Monnet* possa contribuire alla conoscenza e alla comprensione di queste tematiche che sono oggi centrali perché condizionano la vita quotidiana di ciascun individuo.

Il Mercato Unico Digitale quale nuova frontiera dell'integrazione europea. Considerazioni introduttive

DI BRUNO NASCIMBENE [*]

Svolgo alcune considerazioni introduttive alla tavola rotonda dedicata al mercato unico digitale, inteso quale possibile nuova frontiera dell'integrazione europea. La domanda da porsi è la seguente: il mercato unico digitale è davvero una frontiera dell'integrazione europea e, in caso positivo, quale è il suo significato?

Il primo profilo che assume rilievo è la definizione di mercato unico. Esso è, sicuramente, una delle più grandi conquiste del processo di integrazione europea. Oggi ci si riferisce al mercato "unico" o al mercato "interno", nel passato ci si riferiva al mercato "comune". Ciò che viene, comunque, sottolineato dagli studiosi del diritto e della storia dell'Unione europea, quale che sia la dizione impiegata, è l'importanza che il mercato interno riveste nel processo di costruzione dell'Unione. Nel TUE vi è un preciso riferimento al mercato interno all'art. 3, par. 3 ("L'Unione instaura un mercato interno"). Il nesso fra mercato interno e concorrenza è espressamente indicato nel Protocollo n. 27 sul mercato interno della concorrenza, ove si afferma che il mercato interno "comprende un sistema che assicura che la concorrenza non sia falsata". Questi riferimenti normativi sono da tenere presenti anche nella materia qui oggetto di esame.

Il secondo profilo che assume rilievo riguarda il rapporto fra mercato digitale e mercato interno. Il mercato digitale è una *species* del *genus* mercato interno, è una specificazione di quel processo di integrazione che riguarda tutti i settori dell'economia, e non solo. È dunque corretto estendere i rilievi e considerazioni sul mercato interno al mercato digitale, sottolineandone i profili nuovi, le novità insomma, pur tenendo conto della necessità di realizzare, anche in tale contesto, un'economia più forte, equilibrata ed equa.

Per quanto riguarda le fonti relative al mercato digitale, come emerge dalle relazioni di questo convegno, ha un ruolo specifico la Carta dei diritti fondamentali dell'Unione europea. Nella Carta sono state inserite, per la prima volta, norme ad hoc che riguardano la protezione dei dati personali e la libera circolazione dei dati (art. 8, "Protezione dei dati di carattere personale"). Norme generali sono l'art. 16 TFUE (diritto di ogni persona alla protezione dei dati che la riguardava) e l'art. 39 TUE (in materia di politica estera e di sicurezza comune). Nelle "Spiegazioni" che accompagnano la Carta vengono ricordate varie norme di diritto UE, ma anche l'art. 8 della Convenzione europea dei diritti dell'uomo, da cui l'art. 8 della Carta trae diretta ispirazione.

[*] Professore emerito di diritto dell'Unione europea, Università degli Studi di Milano

Il mercato unico digitale non esisteva quando è nato il mercato unico. Sono ormai trascorsi ventisette anni dalla nascita (1.1.1993) del mercato unico, ed è quindi, più che mai "adulto": il mercato digitale ha origine ben più recenti, la sua nascita potendo collocarsi nel 2015, quando la Commissione propose, in una specifica comunicazione, una strategia per il mercato unico digitale in Europa (COM [2015] final del 6.5.2015). Malgrado la "giovane età", le iniziative promosse in questi anni, e quelle in corso di realizzazione sono davvero numerose (come verrà illustrato nel corso del convegno).

Premesso dunque l'inquadramento del mercato unico digitale nel mercato unico, non v'è dubbio che nel mercato digitale sia presente una caratteristica fondamentale del diritto dell'Unione europea: la realizzazione progressiva. Anche questo mercato, invero, si sta realizzando per tappe grazie all'operato delle istituzioni e degli Stati, che collaborano in maniera più o meno intensa e proficua con le istituzioni.

L'Unione non poteva rimanere indifferente alla trasformazione tanto del "mercato", quanto del commercio. L'Unione non poteva, insomma, non rendersi conto di un fenomeno nuovo riguardante lo scambio online dei beni e servizi, fra cui figurano i dati che (come sottolinea il Prof. Rossi Dal Pozzo), sono beni. E come beni, anche i dati devono poter circolare liberamente. Nei documenti della Commissione e del Parlamento in cui si affronta il tema della strategia, si sottolinea la necessità di quanto sia necessario abolire le barriere di carattere normativo alla libera circolazione, auspicando un "internet per tutti" ovvero (precisa la Commissione nella comunicazione sulla "revisione intermedia dell'attuazione della strategia per il mercato unico digitale". doc. COM [2017] final del 10.5.2017) si deve creare un "mercato unico digitale connesso per tutti", un ambiente stabile e trasparente in cui prevalga il senso di affidabilità, che è elemento essenziale per ottenere la fiducia di imprese e consumatori, pienamente coinvolti in questa realizzazione, non diversamente dalle istituzioni e dagli Stati.

È proprio con riferimento a istituzioni e Stati che è opportuno chiedersi quale è il ruolo delle istituzioni nella formazione di una politica digitale, ma soprattutto se esiste una politica digitale dell'Unione europea che non sia meramente affermata, ma realizzata. La stessa domanda riguarda gli Stati, che non possono perseguire politiche nazionali diverse a seconda della sensibilità e approccio verso il "digitale". Le politiche nazionali vanno armonizzate, gli ostacoli vanno rimossi, come si è fatto nel passato, quando si è realizzata la libera circolazione dei beni e dei servizi.

Risultati positivi, finora ottenuti, sono l'abolizione delle tariffe di roaming, la modernizzazione della protezione dei dati, la portabilità transfrontaliera dei contenuti online, l'accordo per sbloccare il commercio elettronico ponendo fine ai blocchi geografici ingiustificati. La prospettiva è, nel quadro della liberalizzazione e libera circolazione, abbattere le barriere esistenti fra gli Stati membri dell'Unione. Come afferma il Consiglio europeo nelle conclusioni del 7.6.2019, perché si realizzi una vera e propria politica digitale europea bisogna superare le inutili burocrazie ed ostacoli nazionali che impediscono l'innovazione, consentendo a cittadini e imprese (indipendentemente dalla loro dimensione e ubicazione) di trarre vantaggio dalla digitalizzazione.

Il quadro normativo del Mercato unico digitale*

DI GIANDONATO CAGGIANO**

SOMMARIO: 1. La strategia digitale 2015-19. – 2. Le trasformazioni tecnologiche e dei modelli di profitto. – 3. Le piattaforme *online*. – 4. La neutralità della Rete. – 5. Il Codice europeo delle comunicazioni elettroniche. – 6. La regolamentazione delle radiofrequenze. – 7. Territorialità del diritto d'autore e principio del paese di origine. – 8. Le misure contro il *geoblocking*. – 9. La regolamentazione del diritto d'autore. – 10. La direttiva sui servizi audiovisivi. – 11. La ritrasmissione *on line* dei programmi delle emittenti televisive. – 12. Dati personali, non-personali e pubblici. – 13. Il pacchetto "contratti digitali". – 14. La direttiva *omnibus* per la tutela dei consumatori.

1. Il mercato unico è una delle realizzazioni di maggior successo dell'integrazione europea[1]. Il mercato digitale ne costituisce una dimensione che interseca quella dei beni e servizi tradizionali, rappresentando una fascia ad elevato valore aggiunto per i cittadini e le imprese[2]. L'innovazione digitale crea opportunità di sviluppo per la trasformazione di interi settori produttivi sulla base dei nuovi modelli di profitto[3].

Sotto l'impulso della Commissione Junker, la strategia per il Mercato unico digitale è stata finalizzata a rafforzare la libertà di circolazione dei fattori produttivi messa a rischio da nuove barriere regolamentari. A fronte della rivoluzione digitale, la regolamentazione dell'Unione è diventata spesso incompleta o inadeguata con la conseguente necessità di adattamento degli strumenti giuridici sui beni e servizi tradizionali e sulle comunicazioni elettroniche adottate negli ultimi due decenni. Da tale

---

* Relazione integralmente rivista e ampliata, Università di Milano, 16 dicembre 2019.

** Professore ordinario, Università di Roma Tre.

[1] Art. 26, par. 2 TFUE. La rimozione degli ostacoli residuali al suo pieno funzionamento consentirebbe enormi vantaggi economici, v. A. TEASDALE (a cura di), *Un dividendo europeo da duemila miliardi di euro, Mappatura del costo della non-Europa 2019-2024*, EPRS, PE 631.745, aprile 2019.

[2] COM(2010) 245 def., del 19 maggio 2010, Un'agenda digitale europea; COM(2015) 192 final, 6 maggio 2015, Strategia per il mercato unico digitale in Europa; SWD (2015) 100 final, A Digital Single Market Strategy for Europe: Analysis and evidence, 6 maggio 2015; IP/15/4919, Un mercato unico digitale per l'Europa: la Commissione definisce 16 iniziative per realizzarlo, 6 maggio 2015. V. anche COM(2015) 550 final, 28 ottobre 2015, Migliorare il mercato unico: maggiori opportunità per i cittadini e per le imprese.

[3] Per facilitare l'accesso *online* alle informazioni, alle procedure amministrative e ai servizi di assistenza per i cittadini e le imprese, è entrato in funzione uno sportello digitale unico, v. Regolamento (UE) 2018/1724 del Parlamento europeo e del Consiglio, del 2 ottobre 2018, che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE) n. 1024/2012.

esigenza è derivato un programma di azioni legislative che si dimostra, per rilievo e ampiezza, paragonabile a quello del mercato interno del 1992[4].

Com'è noto, la competenza concorrente nel mercato comporta l'applicabilità delle regole nazionali e la capacità per il legislatore interno di legiferare solo sino a quando uno specifico aspetto della materia non è sottoposto compiutamente alla legislazione dell'Unione (*pre-emption*) [5]. In relazione agli aspetti innovativi, i rapporti giuridici su beni e servizi digitali tornerebbero ad essere sottoposti alla frammentazione della normativa nazionale.

Una prima parte della Strategia digitale riguardava l'obiettivo dell'accesso ai mercati digitali: semplificare l'*e-commerce* transfrontaliero; garantire i diritti dei consumatori; rendere più rapide le consegne a domicilio dei prodotti; contrastare il fenomeno del c.d. *geo-blocking*; identificare gli ostacoli alla concorrenza; garantire la neutralità della rete; revisionare le regole sulla trasmissione via satellite e via cavo; armonizzare le aliquote IVA. Una seconda parte riguardava l'innovazione digitale: la regolamentazione delle comunicazioni elettroniche; il quadro dei media audiovisivi e il diritto d'autore; le attività delle piattaforme online; la fiducia nei servizi digitali, in particolare rispetto al trattamento dei dati personali; la sicurezza delle reti e delle tecnologie.

Nell'arco di cinque anni, l'attuazione della Strategia ha colmato molte lacune normative e modernizzato vari strumenti legislativi[6]. Nel documento "Completare un mercato unico digitale sicuro per tutti", la Commissione indica il quadro degli atti legislativi necessari al suo funzionamento. Come dimostra l'Allegato a questo articolo[7], gli atti giuridici previsti sono stati tutti adottati, salva la direttiva *e-privacy*[8]. Tra i più rilevanti occorre ricordare il Codice europeo sulle comunicazioni elettroniche, la direttiva sui servizi media audiovisivi, la direttiva sul diritto d'autore, la direttiva sulla trasparenza delle imprese di intermediazione *online*; infine, la direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS), questione di importanza strategica anche per la sovranità

[4] Alla data del 31 dicembre 1992, fissata dall'Atto unico europeo (1987) per il completamento del mercato interno, era stato adottato oltre il 90% dei circa 300 atti legislativi contemplati nel Libro bianco del 1985.

[5] Art. 4, par. 2, lett. a) TFUE.

[6] COM(2015) 192 final, cit.; COM(2016) 288 final, 25 maggio 2016, Le piattaforme *online* e il mercato unico digitale. Opportunità e sfide per l'Europa; COM(2016) 356 final, 2 giugno 2016, Un'agenda europea per l'economia collaborativa; COM(2016) 587 final, Connettività per un mercato unico digitale competitivo: verso una società dei Gigabit europea; COM(2017) 229 final, 10 maggio 2017, Relazione finale sull'indagine settoriale sul commercio elettronico.

[7] Nei primi due anni, la Commissione ha presentato una serie di proposte riguardanti 16 principali misure individuate, v. COM(2017) 228 final, 10 maggio 2017, sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale Un mercato unico digitale connesso per tutti. Il quadro completo delle proposte è riportato nell'Annex al COM(2018) 320 final, 15 maggio 2018, Completare un mercato unico digitale sicuro per tutti. Contributo della Commissione alla riunione informale dei leader dell'UE sulla protezione dei dati e il mercato unico digitale, 16 maggio 2018.

[8] COM(2017)10 final, 10 gennaio 2017, Proposta di Regolamento del Parlamento europeo e del Consiglio, relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE.

tecnologica dell'Unione[9]. Per l'armonizzazione legislativa è stata utilizzata principalmente la basa giuridica dell'art.114 TFUE[10].

Sul quadro normativo in parola ha un particolare impatto anche il regolamento generale sulla protezione dei dati personali [11] che dovrà essere coordinato con la direttiva *e-privacy* (se e quando sarà adottata)[12]; nonché il regolamento sulla neutralità della Rete[13] che ne detta i principi di utilizzazione, in concordanza con l'opzione dalla FCC degli Stati Uniti durante la presidenza Obama (che aveva affermato il principio di neutralità della Rete), ora in contrapposizione con quella della presidenza[14].

Per una migliore comprensione del tema, vale la pena di ricordare che l'infrastruttura, su cui la tecnologia permette di trasmettere le informazioni, ha come possibili varianti e/o componenti: il cavo coassiale, la fibra ottica, le radiofrequenze, oltre al doppino telefonico in rame[15].

[9] Direttiva (UE) 2016/1148 del 6 luglio 2016 sulla sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS).

[10] L'art. 114 TFUE si applica "se il trattato non dispone diversamente", a conferma del suo carattere generale. L'art. 115 TFUE è applicabile "fatto salvo l'art. 114", in ragione del suo carattere suppletivo. Inoltre, l'armonizzazione delle legislazioni nazionali può avvenire anche in virtù della clausola di flessibilità di cui all'art. 352 TFUE, laddove occorra realizzare uno degli obiettivi fissati dal trattato quando non sono previsti poteri specifici a tal fine. G. GATTINARA, *Artt. 114-115 TFUE*, in C. CURTI GIALDINO (a cura di), *Codice dell'Unione europea operativo*, Napoli, 2012, 1144 ss.; C. AMALFITANO, *Ravvicinamento delle legislazioni [dir. UE]*, in *Treccani, Diritto on line* (2015).

[11] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

[12] COM(2017) 10 final, cit.

[13] Regolamento (UE) 2015/2120 del Parlamento europeo e del Consiglio, del 25 novembre 2015, che stabilisce misure riguardanti l'accesso a un'Internet aperta e le tariffe al dettaglio per le comunicazioni intra-UE regolamentate e che modifica la direttiva 2002/22/CE e il regolamento (UE) n. 531/2012.

[14] La nuova FCC nominata sotto la presidenza Trump ha revocato tale decisione alla fine del 2017, confermata dalla D.C. Circuit Court of Appeals, il 7 ottobre 2019. Una legge che mira a ripristinare la neutralità della Rete (Save the Internet Act) approvata dal Congresso non ha molte speranze di passare al Senato.

[15] Molti Stati membri dispongono di una duplice infrastruttura fissa (cavo coassiale e rete a fibre ottiche). Dal punto di vista tecnico la Banda Ultra Larga (*Ultra-broadband*) consente una velocità di connessione in ricezione (*download*) di almeno 30 Mbps (NGA, *Next Generation Access*). L'infrastruttura rilevante per gli attuali sviluppi tecnologici è costituita dalle reti VHCN (*Very High Capacity Networks*) con una velocità di connessione molto maggiore di 100 Mbps tendente ad un Giga. Secondo la definizione della Commissione europea, la rete del doppino telefonico di rame di cui dispone l'Italia, almeno sino alla realizzazione completa della rete a fibre ottiche, non è classificabile tra le reti VHCN; neanche nella versione ibrida con la rete in fibra -VDSL (dalla centrale sino agli armadi stradali sulla fibra con l'ultimo miglio sul doppino in rame), dal momento che la velocità massima così raggiungibile (100 sino a 200 Mbps) dipende dalla distanza armadio stradale/terminale dell'utente.

2. Il quadro normativo attuale è il risultato della liberalizzazione dei servizi delle telecomunicazioni[16] e della regolazione *ex-ante* della rete dell'ex-monopolista negli anni '90, sino al pacchetto di direttive sulle comunicazioni elettroniche del 2002 (modificate nel 2009). La liberalizzazione del mercato delle telecomunicazioni è stata ottenuta in due fasi della regolazione della Rete dell'ex-monopolista: la prima sul diritto di accesso alla Rete a costi e livelli di qualità uguali per tutti i fornitori; la seconda sul diritto di accesso disaggregato alla Rete (*unbundling*).

Il funzionamento attuale delle comunicazioni elettroniche vede come protagonisti attori diversi da quelli che operano nei mercati tradizionali. Gli Internet Service Provider (ISP), connessi a una infrastruttura fissa e/o mobile (metallica, in fibra, su frequenze radio) forniscono l'accesso alla Rete su cui si svolge il passaggio delle comunicazioni elettroniche. L'ISP ha rapporti, a monte, con l'operatore dell'infrastruttura e, a valle, con gli acquirenti di capacità trasmissiva, utenti diretti o fornitori (a loro volta di servizi agli utenti). Nello scenario è diventata preponderante, in termini di profitto, la presenza di soggetti "over the net" (OTT), che offrono servizi ed applicazioni di vario genere, utilizzando la Rete di cui comprano la capacità trasmissiva. Tra questi operano le piattaforme *online,* imprese intermediarie che offrono un'architettura digitale commerciale per le interazioni online tra altre aziende/professionisti e utenti/consumatori. In sostanza, la struttura multi-versante delle piattaforme è impostata in modo da consentire sia le transazioni contrattuali tra professionisti-terzi e consumatori, sia la vendita diretta di prodotti, servizi e contenuti digitali[17].

Da questo affollamento di attori deriva la necessità di ottimizzare la capacità trasmissiva della Rete, fissando regole limitative in caso di sua eventuale congestione tecnica e/o per utilizzazione tramite specifiche applicazioni particolarmente ingombranti (IPTV, musica in *streaming* a costo zero). Per evitare un possibile caos della Rete attuale, gli sviluppi del 5G bisognosi di banda ultra-larga impongono investimenti della capacità trasmissiva (duplicazione, co-investimenti o cooperazione per/nella rete a fibre ottiche) e

[16] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno.

[17] I modelli commerciali delle piattaforme comprendono: motori di ricerca, ad es. Google, Yahoo!; social Media, ad es. Facebook, Twitter; strumenti di recensione degli utenti per es. Tripadvisor; strumenti di confronto, ad es. Trivago.com, Rentalcars.com, Kayak.com, Booking.com; piattaforme dell'economia collaborativa, ad es. Airbnb, Uber, BlaBlaCar; piattaforme di commercio elettronico (mercati), ad es. Zalando, Amazon, Alibaba, Ebay; negozi di App, ad es. Apple App Store, Google Play, Amazon App Store; siti Internet di acquisto collettivo, ad es. Groupon. In dottrina, v. *inter alia*, K.A. BAMBERGER-O. LOBEL, *Platform market power*, 2018; J. M. NEWMAN, *Complex antitrust harm in platform markets*, 2017; R. FRIEDEN, *The internet of platforms and two side-markets: implication for competition and consumers*, 2017 (reperibili *online*). V. gli ultimi rapporti a livello dell'Unione, del Regno Unito e degli Stati Uniti: EC SPECIAL ADVISERS REPORT, *Competition Policy for the Digital Era* (April 2019); J. FURMAN ET AL., *Unlocking Digital Competition, Uk Report of the Digital Competition Expert Pane*l, 13 March 2019; STIGLER COMMITTEE ON DIGITAL PLATFORMS, *Final Report*, The University of Chicago Booth School of Business, 16 September 2019.

lo sviluppo di radiofrequenze, secondo le regole stabilite dal Codice europeo delle comunicazioni elettroniche[18]. Il cambiamento e la modernizzazione del contesto normativo rappresentano fattori fondamentali per gli investimenti nello sviluppo della Rete, oltre all'uso di fondi pubblici nell'ambito del regime di aiuti di Stato[19].

La prospettiva della politica di concorrenza, il cui approfondimento non può essere svolto in questa sede, si riferisce a specifici mercati digitali per ciascuna tipologia di attività la cui identificazione richiede l'analisi di mercato geografico e per prodotto. L'economia digitale ha modificato molti mercati e i fattori lesivi della concorrenza, determinando il fenomeno della personalizzazione di massa e una nuova catena del valore per molte imprese (modelli di profitto, processo, network e struttura). Nel caso delle misure antitrust occorre verificare gli eventuali comportamenti abusivi/restrittivi dell'impresa in posizione dominante; nel caso degli interventi regolatori, la valutazione del possesso di un significativo potere di mercato (SPM) per l'imposizione ex-ante di eventuali misure asimmetriche.

Al riguardo, nel dibattito istituzionale si pone la questione se gli interventi antitrust debbano avere un ruolo centrale ed esaustivo o se, invece, non debbano essere integrati dagli interventi della regolazione. Com'è noto, i due set di strumenti della concorrenza e della regolazione, pur se con tempi e modalità diverse, convergono ai fini di conservare o produrre condizioni tali che consentano ai mercati di diventare o di continuare ad essere equi e contendibili per gli innovatori e, in generale, per i nuovi entranti/competitori capaci. Molti ritengono preferibile un controllo più rigoroso nei confronti delle condotte delle imprese con significativo potere di mercato (SPM) tramite interventi di natura regolamentare *ex-ante,* ivi compresa la costituzione di una nuova Autorità regolamentare europea *ad hoc*. Gli interventi antitrust *ex-post* e le sanzioni pecuniarie anche dell'ordine di miliardi di euro appaiono inidonei a correggere gli abusi di posizione dominante nei mercati digitali, considerate le disponibilità finanziare dei Giganti digitali (Big Tech). Salvo se si modificassero le soglie di valutazione nel caso di acquisizioni, gli interventi riguardano comportamenti passati e talvolta già obsoleti.

Ci si interroga se l'economia delle piattaforme digitali non sia in una situazione a rischio di *forclosure* dei mercati relativi, tale da richiedere una politica dell'Unione *ad hoc* della stessa intensità di quella che portò alla liberalizzazione a partire dagli anni '90. In ogni caso, le caratteristiche attuali dei mercati digitali mettono in discussione molti temi: l'efficacia del metodo utilizzato per l'analisi del mercato (1997): la caratteristica multi-versante di alcuni mercati, il loro effetto di rete, la centralità dei Big Data, la diffusione degli algoritmi (con la possibilità di discriminazione e profilazione), l'accresciuta facilità della "collusione senza intesa fra le parti" in mercati oligopolistici.

[18] V. anche Direttiva 2014/61/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, recante misure volte a ridurre i costi dell'installazione di reti di comunicazione elettronica ad alta velocità.

[19] Sul regime di aiuti di Stato per l'infrastruttura a banda larga, v. R. FEASEY, M. BOURREAU, A. NICOLLE, *State Aid for Broadband Infrastructure in Europe*, CERRE 5/126, November 2018.

Specie in occasione del controllo delle concentrazioni non v'è dubbio che sia necessario un ripensamento della valutazione degli aspetti strutturali del processo competitivo[20].

3. La direttiva 2000/31/CE sui servizi della società dell'informazione (direttiva sul commercio elettronico) [21] ha lo scopo di promuovere lo sviluppo senza ostacoli dei fornitori di accesso al web, offrendo in cambio agli operatori - *Internet service provider*, ISP -, un favorevole regime di responsabilità per lo sviluppo delle attività sulla Rete. Vent'anni fa, tale direttiva ha posto le basi del mercato unico digitale fissando il principio del paese d'origine, vietando qualsiasi forma di autorizzazione preventiva, istituendo un regime di responsabilità limitata e un divieto generale di sorveglianza dell'ISP. Al tempo, si trattava di un contesto pioneristico che richiedeva promozione e sostegno per attività che erano ancora allo stato iniziale. Una ragione del successo della direttiva in parola è stata la sua formulazione neutra dal punto di vista tecnologico che ha così evitato la necessità di modifiche a seguito dell'innovazione digitale. Il sistema ha funzionato bene, anche grazie ai chiarimenti della giurisprudenza della Corte di giustizia.

Ora, tale regime, se non del tutto obsoleto, richiede una modernizzazione.

L'evoluzione dello sviluppo e dell'uso di piattaforme *online* per una vasta serie di attività rende difficile elaborare un'unica definizione di piattaforme *online*. Insostenibile appare la tesi che i tutti i servizi erogati dalle piattaforme rientrino generalmente nella speciale categoria di servizi della "società dell'informazione" creata nel 2000 dalla direttiva *e-commerce*[22]. Le loro attività vanno oggi ben oltre la funzione di strumenti passivi di trasmissione e di archiviazione, una caratteristica che giustificava, un tempo, le esenzioni dalla responsabilità per i contenuti di terzi e l'assenza di un obbligo generale di monitoraggio[23].

Il completamento del mercato unico digitale richiede una maggiore trasparenza per le attività commerciali svolte tramite le piattaforme *online*. Il regolamento 2019/1150[24]

[20] E. ARGENTESI, P. BUCCIROSSI, E. CALVANO, T. DUSO, A. MARRAZZO, S. NAVA, *Ex-Post Assessment of Merger Control Decisions in Digital Markets*, in *CESifo Working Paper*, June 2019.

[21] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico"). Secondo la definizione più recente: (…) servizio della società dell'informazione, è "qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi", v. Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche delle regole relative ai servizi della società dell'informazione.

[22] N. IACOB, F. SIMONELLI, *How to Fully Reap the Benefits of the Internal Market for E-Commerce? New economic opportunities and challenges for digital services 20 years after the adoption of the e-Commerce Directive*, EP STUDY, Requested by the IMCO committee PE 648.801, May 2020.

[23] COM(2017) 555 final, 28 settembre 2017, Lotta ai contenuti illeciti *online*. Verso una maggiore responsabilizzazione delle piattaforme *online*.

[24] Il Regolamento dispone che i termini e le condizioni d'uso unilateralmente predisposti dalle piattaforme debbano essere redatti in un linguaggio semplice e comprensibile ed essere facilmente

comprende i mercati *online*, gli *store* di applicazioni *software online* e/o i *social media*, nonché i motori di ricerca, indipendentemente dal luogo di ubicazione, purché servano gli utenti commerciali e i consumatori stabiliti nell'Unione. A favore degli utenti commerciali ("il professionista"), il regolamento stabilisce una serie di obblighi in capo ai "fornitori di servizi di intermediazione *online*" (*Platform to Busine*ss, P2B). I principali obblighi riguardano: la chiarezza nella redazione dei termini e delle condizioni; la comunicazione appropriata agli utenti di qualunque modifica di tali termini e condizioni; la previsione di meccanismi di comunicazione per limitazioni, sospensioni o cessazioni dei servizi; nonché la fissazione dei principali parametri che determinano il posizionamento di un certo prodotto/servizio, che debbono essere motivati.

In molti casi le piattaforme non forniscono informazioni sufficienti, esercitando una discrezionalità assoluta ed il potere di modificare l'ordine di presentazione dei prodotti sulla base di motivazioni spesso assai vaghe, quali ad es. la popolarità. Le scelte operate al riguardo incidono significativamente sulle scelte dei consumatori.

Nel caso in cui sia il fornitore di servizi di intermediazione *online* a offrire determinati beni o servizi ai consumatori attraverso i suoi stessi servizi, il regolamento 2019/1150 riconosce che il fornitore può utilizzare il proprio controllo per garantire alle proprie offerte, o a quelle di un utente commerciale controllato, vantaggi tecnici o economici a svantaggio di utenti commerciali concorrenti, compromettendo così la concorrenza leale e limitando le possibilità di scelta dei consumatori. Tuttavia, simili pratiche non sono oggetto di restrizioni, il Regolamento si limita a stabilire che il fornitore dei servizi di intermediazione *online* debba agire in maniera trasparente fornendo una descrizione e un esame appropriati per eventuali trattamenti differenziati, attraverso mezzi legali, commerciali o tecnici. Simili disposizioni rischiano di avere un'efficacia molto limitata, anche in ragione dei limiti posti all'estensione di tali obblighi in nome della tutela del segreto commerciale[25]. Il sistema normativo segue la giurisprudenza della Corte di giustizia, in particolare le sentenze *Google France SARL* e *eBay* e *L'Orèal*[26].

Per quanto riguarda i meccanismi di ricorso, il regolamento obbliga tutte le piattaforme a istituire un sistema interno di gestione dei reclami efficace e rapido, ivi compresi organismi composti da mediatori specializzati indipendenti. Richiede di indicare uno o più mediatori per i casi in cui il sistema interno di gestione dei reclami non

reperibili. Il Regolamento obbliga altresì la piattaforma a dare comunicazione preventiva al professionista della decisione di limitare o sospendere la fornitura del servizio di intermediazione, indicando le motivazioni.

[25] Direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti.

[26]Sentenze del 23 marzo 2010, cause riunite da C-236/08 a C-238/08, *Google France*, ECLI:EU:C:2010:159, punti 106-120; del 12 luglio 2011, causa C-324/09, *L'Oréal SA,* ECLI:EU:C:2011:474. Sul sistema di posizionamento pubblicitario, v. anche le sentenze 25 marzo 2010, causa C-278/08, *BergSpechte*, ECLI:EU:C:2010:163, punti da 5 a 7; 8 luglio 2010, causa C-558/08, *Portakabin e Portakabin*, ECLI:EU:C:2010:416, punti da 8 a 10; 22 settembre 2011, causa C-323/09, *Interflora Inc. e Interflora British Unit*, ECLI:EU:C:2011:604, punti da 9 a 13.

sia in grado di risolvere una controversia tra i loro utenti commerciali. Il regolamento sancisce il diritto delle organizzazioni rappresentative, associazioni e organismi pubblici di promuovere procedimenti giudiziari nei confronti delle piattaforme; conferisce infine agli Stati membri il potere di stabilire sanzioni in conformità dei sistemi nazionali in caso di violazione del regolamento.

A seguito delle contrastanti sentenze della Corte di giustizia, *Uber* e *Airbnb*[27], si può affermare che i poteri delle piattaforme vanno configurati in relazione al servizio sottostante fornito. Con la più recente sentenza, la Corte è stata chiamata a valutare se l'attività svolta dalla piattaforma potesse essere qualificata come servizio della società dell'informazione oppure se fosse qualificabile come una particolare forma di prestazione di servizi di intermediazione immobiliare. L'elemento preponderante del servizio è stato individuato nella creazione di una lista degli alloggi disponibili, ordinati per criteri impostati dagli utenti, volta ad agevolare il contatto tra domanda ed offerta ma distinta dall'operazione immobiliare conclusa dagli utenti.

4. Con il regolamento (UE) 2015/2120, l'Unione ha stabilito il principio di un'Internet aperta[28]. Il principio di base è quello che gli utenti finali dei servizi di accesso a Internet hanno il diritto di accedere a informazioni, contenuti, applicazioni e servizi di loro scelta e di diffonderli (articolo 3, par. 1). Gli accordi tra i fornitori di servizi di accesso a Internet e gli utenti finali non devono limitare l'esercizio dei diritti degli utenti finali (ivi, par. 2)[29]. La gestione del traffico (bloccare, rallentare, alterare, limitare,

[27] La Corte di giustizia ha statuito che la società Uber esercitava un'influenza decisiva sulle condizioni della prestazione di trasporto degli autisti non professionisti che fanno uso dell'applicazione messa a loro disposizione da detta società, v. sentenze del 20 dicembre 2017, *Asociación Profesional Elite Taxi*, C-434/15, EU:C:2017:981, punto 39, e del 10 aprile 2018, *Uber France*, C-320/16, EU:C:2018:221, punto 21. Per AirBnB, si veda la sentenza del 9 dicembre 2019, causa C-390/18, *AirBnB Ireland*. Per approfondimenti, v. S. BASTIANON, *UberPop è un servizio di trasporto: la prima pronuncia della Corte di giustizia*, in *Eurojus*, 2018, p. 1 ss.; D. DIVERIO, *Se Uber-pop è un servizio di trasporto un via libera condizionato alla sua regolamentazione da parte degli Stati membri*, in *Riv. it. dir. lav.*, 2018. p. 410 ss; M. COLANGELO, M. MAGGIOLINO, *Uber and challenges for antitrust law and regulation*, in *Medialaws*, 2018, p.176 ss.; M. FINCK, *Distinguishing Internet Platforms from Transport Services: Elite Taxi v. Uber Spain*. in *CML Rev*, 2018, p. 1619 ss.; V. HATZOPOULOS, *After Uber Spain: the EU's Approach on the Sharing Economy in Need of Review?* in *European Law Rev.*, 2019, p. 88 ss.; M. INGLESE *Affinità e divergenze fra le sentenze Elite Taxi e Airbnb Ireland*, in *Eurojus*, 2020/1, p. 37 ss.

[28] Regolamento (UE) 2015/2120, cit.; COM (2019) 203 final, 30 aprile 2019, Relazione sull'attuazione delle disposizioni del regolamento (UE) 2015/2120 in materia di accesso a un'Internet aperta. Per un'analisi, v. G. DE MINICO, *Net-neutrality come diritto fondamentale di chi verrà*, in *Costituzionalismo*, 1, 2016; M. OROFINO, *La declinazione della net-neutrality nel Regolamento europeo 2015/2120. Un primo passo per garantire un'Internet aperta*? In *federalismi.it* 2/2016.

[29] "Gli accordi tra i fornitori di servizi di accesso a Internet e gli utenti finali sulle condizioni e sulle caratteristiche commerciali e tecniche dei servizi di accesso a Internet quali prezzo, volumi di dati o velocità, e le pratiche commerciali adottate dai fornitori di servizi di accesso a Internet non limitano l'esercizio dei diritti degli utenti finali (…)" (art. 3, par. 2). Pertanto, gli utenti finali

interferire con, degradare o discriminare tra specifici contenuti, applicazioni o servizi) per l'ottimizzazione della qualità dei servizi trasmessi è consentita purché sia ragionevole.

Il divieto del blocco e della restrizione di contenuti, applicazioni e servizi nonché la discriminazione tra gli stessi prevede solo alcune limitate eccezioni (ivi, par. 3), restrittive al fine di conformarsi ad atti legislativi, preservare la sicurezza delle reti o prevenire una congestione della rete eccezionale/temporanea. Si tratta della norma base della neutralità della rete. Esso prevede infatti che gli ISP, nel fornire i servizi di accesso ad Internet, debbano trattare tutto il traffico allo stesso modo, senza discriminazioni, restrizioni o interferenze. Tuttavia, la previsione è temperata dalla definizione di gestione del traffico ragionevole, basata non su considerazioni di ordine commerciale, ma solo su requisiti di capacità tecnica del servizio, obiettivamente diversi per specifiche categorie di traffico[30]. Sarebbe invece irragionevole ad esempio un'offerta *zero rating*[31] che , al raggiungimento del limite di traffico, comportasse il blocco o il rallentamento di tutte le altre applicazioni. In ogni caso, le misure di gestione del traffico devono essere conformi ai principi di necessità e di proporzionalità per quanto riguarda il trattamento dei dati personali e al relativo quadro di riferimento dell'Unione in materia (ivi, par. 4). La regolamentazione favorisce la trasparenza per quanto concerne le condizioni contrattuali per i servizi di accesso a Internet per gli utenti finali e le informazioni che i fornitori di servizi Internet pubblicano nei loro siti web (art. 4, par. 1).

I fornitori di servizi Internet possono fornire servizi specializzati (diversi dai servizi di accesso a Internet) ottimizzati per specifici contenuti, applicazioni o servizi, al fine di soddisfare i requisiti un livello specifico di qualità, solo a condizione che la capacità della rete sia sufficiente per tutti senza peggiorarne la qualità dei normali servizi di accesso (ivi, par. 5)[32]. Si tratta soprattutto di servizi di gestione chiamate (VoIP) e servizi per la televisione (IPTV), ma si prevedono nuovi servizi specializzati, incentivati dalle reti 5G che porranno alle ANR una questione di interpretazione di questa condizionalità. Il rischio paventato da alcuni operatori è che per verificare il presupposto tecnico sia

hanno il diritto di scegliere prezzi differenti per parametri di qualità del servizio diversi (ad esempio volumi di dati o velocità). La protezione dei consumatori che hanno acquistato servizi di qualità inferiore è garantita dalle misure di trasparenza delle condizioni e dei contratti (art. 4).

[30] V. BEREC, Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, BoR (16) 127, 30 agosto 2016, punti 58-61.

[31] Un'offerta si dice "zero rating" quando un fornitore di servizi Internet applica un prezzo marginale pari a zero al traffico di dati relativo a una specifica applicazione o categoria di applicazioni (e i dati consumati non vengono computati ai fini del raggiungimento di un certo limite di traffico). Tali offerte hanno minore probabilità di creare effetti distorsivi sul mercato dei contenuti nei casi in cui comprendano intere categorie di applicazioni (ad esempio tutti i servizi di *streaming* musicali), piuttosto che nel caso in cui includano una serie limitata di applicazioni.

[32] L'ottimizzazione riguarda la fornitura di un accesso ad Internet qualitativamente superiore per quei servizi che necessitano ampiezza di banda e velocità. In proposito, i fornitori di comunicazione elettronica, inclusi gli ISP e i fornitori di contenuti, applicazioni e servizi "sono liberi di offrire servizi diversi dai servizi di accesso a Internet ottimizzati per specifici contenuti, applicazioni o servizi o loro combinazioni, nei casi in cui l'ottimizzazione sia necessaria per soddisfare i requisiti relativi a contenuti, applicazioni o servizi per un livello specifico di qualità" (art. 3, par. 5, 1° sub par.).

necessario ottenere un'autorizzazione prima del lancio del servizio specializzato. D'altro canto, la crescita incontrollata mette a rischio la flessibilità da offrire agli utenti finali che permetta di trarre beneficio dall'assegnazione dinamica delle risorse, senza una occupazione della capacità trasmissiva da parte dei servizi specializzati, a scapito della qualità generale dei servizi di accesso alla Rete.

Nell'assetto complessivo assumono importanza centrale le Autorità nazionali di regolamentazione (art. 5), con il compito di monitorare il rispetto della normativa, promuovere la disponibilità di accesso indiscriminato di qualità e imporne requisiti minimi nel servizio. La vigilanza si svolge sia *ex ante,* come possibilità di richiedere agli operatori le informazioni inerenti la loro capacità trasmissiva, il traffico e le eventuali misure tecniche di gestione adottate, sia *ex post,* come attività di controllo e monitoraggio delle restrizioni ai diritti degli utenti, delle condizioni contrattuali e delle pratiche commerciali, delle operazioni di gestione del traffico, dell'impatto dei servizi ottimizzati sulla qualità generale dei servizi di accesso e dei requisiti di trasparenza imposti agli ISP.

I rischi per gli operatori di rete e per la loro libertà di impresa, che si produrrebbero in assenza di investimenti sull'aumento della capacità trasmissiva tramite reti di nuova generazione, potrebbero essere compensati proprio dalla trasmissione di servizi ottimizzati[33]. Infine, il regolamento riconosce agli utenti finali il diritto di utilizzare l'apparecchiatura terminale di loro scelta per evitare discriminazioni all'accesso alla rete sulla base del terminale o del sistema operativo utilizzato[34] .

La Corte di Giustizia ha statuito sull'interpretazione dei principi della neutralità della Rete e in ordine alle misure possibili (ad es. non può essere richiesta ad essi una funzione di filtro e monitoraggio automatico sui contenuti[35] in relazione alle questioni inerenti la tutela della proprietà intellettuale. Si tratta di un difficile bilanciamento tra la tutela del diritto d'autore e la liberà di impresa degli ISP che assumono una responsabilità, anche se sono terzi rispetto agli atti di contraffazione commessi dai loro utenti.

[33] V. in proposito la Raccomandazione 2010/572/CE della Commissione relativa all'accesso regolamentato alle reti di nuova generazione del 20 settembre 2010, nonché la Raccomandazione 2014/710/UE del 9 ottobre 2014, relativa ai mercati rilevanti di prodotti e servizi del settore delle comunicazioni elettroniche che possono essere oggetto di una regolamentazione ex ante ai sensi della direttiva 2002/21/CE del Parlamento europeo e del Consiglio che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica,

[34] Cosi è possibile usare il *tethering* per realizzare un terminale con lo *smartphone* oppure usare *whatsapp* sullo *smartphone* o sul computer.

[35] La direttiva 2001/29/CE (art. 8, par. 3) che prevede la facoltà per i titolari dei diritti di chiedere un provvedimento inibitorio nei confronti dell'intermediario i cui servizi sono utilizzati per violare il diritto d'autore, V. sentenze 24 novembre 2011, *Sabam I* ECLI:EU:C:2011:771; 16 febbraio 2012, *Sabam II*, ECLI:EU:C:2012:85; 27 marzo 2014, causa C-314/12, *UPC Telekabel*, ECLI:EU:C:2014:192 (limiti alle misure cautelari di interruzione di accesso ad un sito internet); 8 settembre 2016, causa C- 160/15, *GS Media* (in merito a *link* non autorizzati che consentivano l'accesso a contenuti digitali di terzi protetti dal diritto d'autore).

Gli Orientamenti del Gruppo europeo dei regolatori (di seguito: BEREC)[36], forniscono indicazioni per l'attuazione delle regole europee da parte delle ANR, in particolare, con riferimento a: pratiche commerciali e negoziali, ivi incluse le pratiche di *zero-rating*; misure di gestione del traffico; fornitura di servizi specializzati; valutazione delle misure di trasparenzza nei contratti per la fornitura di accesso alla Rete agli utenti.

5. Il nuovo Codice delle comunicazioni elettroniche, insieme al regolamento (UE) 2018/1971 relativo al BEREC[37], disciplina unitariamente le reti e i servizi[38]. Rispetto al precedente pacchetto normativo, è stata "scorporata" solo la direttiva relativa alla vita privata e alle comunicazioni elettroniche (*e-privacy*)[39]. Il Codice ha definito un nuovo e prioritario obiettivo, vale a dire la promozione della connettività e dell'accesso alle reti ad altissima capacità in un contesto normativo favorevole a nuovi investimenti.

Per quanto riguarda l'ambito di applicazione, il Codice introduce la nozione di servizio di comunicazione interpersonale (art. 2) che comprende anche gli operatori *over the top* (OTT), sia pure con intensità diversa a seconda che utilizzino o meno risorse di numerazione[40]. Resta fermo il regime di autorizzazione generale per le reti di comunicazione elettronica e i servizi di comunicazione elettronica senza bisogno di una decisione amministrativa, ma solo di una notifica dichiarativa. Le modifiche hanno lo scopo di estendere alcune garanzie normative esistenti, ad esempio in relazione alla crittografia dei messaggi (art. 40) e alla pubblicazione di informazioni per gli utenti (articoli 102-104). In particolare, "i surrogati più vicini" della telefonia tradizionale e dei

[36] BEREC, Guidelines on the Implementation, cit. A tal fine, il BEREC ha svolto una consultazione pubblica; Consultation paper on the evaluation of the application of Regulation (EU) 2015/2120 and the BEREC Net Neutrality Guidelines, BoR (18); BEREC Report on the outcome of the consultation on the evaluation of the application of Regulation (EU) 2015/2120 and the BEREC Net Neutrality Guidelines", BoR (18) 245. V. anche, BEREC Opinion for the evaluation of the application of Regulation (EU) 2015/2120 and the BEREC Net Neutrality Guidelines, BoR (18) 244.

[37] Il Codice introduce inoltre una procedura per l'identificazione di mercati transnazionali, affidando al BEREC la relativa competenza.

[38] Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche, che ha rifuso le direttive del Parlamento europeo e del Consiglio del 7 marzo 2002: 2002/19/CE (direttiva accesso); 2002/20/CE (direttiva autorizzazioni), 2002/21/CE (direttiva quadro), 2002/22/CE, (direttiva servizio universale). Rientrano nell'ambito di applicazione del Codice anche i cosiddetti "servizi di comunicazione interpersonale" che consentono lo scambio interpersonale e interattivo di informazioni, come posta elettronica, i servizi di messaggistica o le chat di gruppo, VoIP Servizi di comunicazione interpersonale indipendenti da numero, ovvero quelle applicazioni che utilizzano il numero come identificativo.

[39] COM(2017) 10 final, cit.

[40] Queste disposizioni hanno lo scopo di garantire che nell'ambito del Codice rientrino servizi come WhatsApp o servizi di messaggistica digitale simili che rappresentano sostituti funzionali dei servizi di telecomunicazione tradizionali come la telefonia vocale o SMS pur mantenendo una gerarchia "a due livelli" di obblighi normativi, con obblighi più onerosi per quei servizi interpersonali che richiedono numeri di telefono (e quindi appaiono più simili ai servizi tradizionali offerti dagli operatori) e obblighi meno onerosi per quelli che non lo fanno.

servizi SMS sono tenuti agli stessi obblighi normativi aggiuntivi (come fornire accesso ai servizi di emergenza, art. 109; servizi di consultazione degli elenchi, art. 112)). In prospettiva è possibile un ulteriore allineamento fra le due tipologie, come il contributo dei fornitori di servizi di piattaforme digitali ai costi degli obblighi di servizio universale (art. 90). Al contempo, il Codice cerca di distribuire l'onere normativo in modo proporzionale alla dimensione dei soggetti e degli interessi meritevoli di tutela. Sono esentate da molti degli obblighi previsti le "microimprese" che forniscono servizi di comunicazione interpersonale "indipendenti dal numero" (art. 98). Al contrario, alcune misure per i consumatori sono soggette alla "massima armonizzazione" (art. 101), senza margini di discrezionalità da parte degli Stati membri, tranne che per un periodo transitorio o in relazione a misure preesistenti che siano obiettivamente giustificabili.

Il Codice inoltre aggiorna e ridefinisce il regime normativo in capo ai fornitori di servizi di comunicazione elettronica.

Per gli obblighi di servizio universale, elimina servizi ormai obsoleti, come i telefoni pubblici a pagamento, gli elenchi abbonati e il servizio di consultazione degli elenchi. In base al nuovo regime, gli Stati membri sono tenuti ad assicurare a tutti i consumatori nei loro territori l'accesso a prezzi abbordabili a un adeguato servizio di accesso a internet a banda larga e a servizi di comunicazione vocale, che siano disponibili, al livello qualitativo specificato nei loro territori, in postazione fissa. Riguardo alla tutela dei consumatori, il Codice impone nuovi obblighi di trasparenza in relazione alle condizioni, ai prezzi e alla qualità dei servizi di comunicazione elettronica e prevede il diritto degli utenti finali di accedere gratuitamente ad almeno uno strumento di confronto dei diversi servizi offerti.

Una parte rilevante del Codice riguarda la regolazione *ex-ante*. Le ANR hanno un obbligo di promuovere l'accesso e la diffusione delle reti ad altissima capacità (art. 3)[41]. Quanto alla regolazione dell'accesso, si assiste ad un ampliamento dei poteri delle autorità nazionali di regolazione di imporre obblighi di accesso simmetrici (i.e. imposti a tutti gli operatori) in presenza di elementi di rete non replicabili. In tali casi, il Codice consente di imporre l'accesso al cablaggio e alle risorse correlate all'interno degli edifici o fino al primo punto di concentrazione o di distribuzione, se situato fuori dall'edificio. In generale, risulta rafforzato il principio per cui gli obblighi relativi all'accesso devono essere proporzionati e sono imponibili solo laddove risulti necessario nell'interesse dell'utente finale o per ovviare a situazioni di effettivo fallimento del mercato al dettaglio.

[41] "Una rete di comunicazione elettronica costituita interamente da elementi in fibra ottica almeno fino al punto di distribuzione nel luogo servito oppure una rete di comunicazione elettronica in grado di fornire prestazioni di rete analoghe in condizioni normali di picco in termini di larghezza di banda disponibile per *downlink/uplink*, resilienza, parametri di errore, latenza e relativa variazione (…)". Per rete a banda ultralarga ci si riferisce a una connessione in fibra ottica o ad un'altra di prestazioni analoghe, quindi anche radio. Il Codice non indica valori numerici minimi circa la velocità di connessione. La proposta del BEREC è quella di definire una "rete a banda ultralarga", secondo criteri non esclusivi che riguardano il tipo di connessione ma anche le prestazioni complessive delle connessioni fisse e senza fili (1 Gbps/200 Mbps e di 150 Mbps/50 Mbps).

Per la regolazione asimmetrica per gli operatori con significativo potere di mercato (SPM), l'impostazione generale non cambia anche se viene esteso il termine per il rinnovo delle analisi di mercato (da tre a cinque anni). Tuttavia, la novità più significativa è rappresentata dalla riduzione del carico regolatorio, in presenza di determinate condizioni, per gli operatori che si impegnino ad aprire al co-investimento per la realizzazione di una nuova rete ad altissima capacità, nonché per gli operatori attivi esclusivamente sul mercato all'ingrosso dei servizi di comunicazione elettronica (*wholesale only*). La concorrenza basata sulle infrastrutture deve essere perseguita solo nella misura in cui sia "efficiente", quando altri mezzi siano possibili per promuovere gli investimenti, cercando di evitare la duplicazione delle risorse di rete. Per evitare duplicazioni si prevedono altre misure, come il co-investimento in un'infrastruttura comune (art. 76) e l'obbligo di fornire un accesso "simmetrico" alle strutture locali (art. 61). Ciò potrebbe implicare un significativo spostamento dalla concorrenza tra soggetti proprietari di rete separate, verso un grado più ampio di condivisione e cooperazione tra operatori. Nella versione più radicale, gli operatori potrebbero superare le misure comportamentali e intraprendere una separazione strutturale delle loro risorse di rete dalle loro operazioni di vendita al dettaglio, al fine di beneficiare di una ridotta supervisione regolatoria (articoli 78 e 80).

Le ANR avranno il compito di sovrintendere a una serie di nuovi fornitori di servizi di comunicazione, alcuni dei quali potrebbero non avere alcuna presenza all'interno dello Stato membro in questione. Le ANR potranno imporre, in casi giustificati, obblighi di interoperabilità ai fornitori di servizi di comunicazione interpersonale "indipendenti dal numero", se essi hanno un "livello significativo di copertura e assorbimento da parte dell'utente" (art. 61, par. 2, lett. c)). La condizione per l'imposizione di tali obblighi è che la Commissione abbia riscontrato una minaccia all'interoperabilità tra utenti in almeno tre Stati membri.

6. La Codice contiene, tra l'altro, regole sul coordinamento dello spettro radio tra gli Stati membri e armonizza le regole sulla sua gestione e l'utilizzo condiviso dello spettro radio. La risorsa dello spettro radio ha un'importanza crescente per lo sviluppo della società digitale[42] e la disponibilità di un idoneo quantitativo di spettro radio rappresenta

[42] La decisione n. 243/2012/UE del 14 marzo 2012 che istituisce un programma pluriennale relativo alla politica in materia di spettro radio stabiliva una politica in materia di spettro radio per la pianificazione strategica nel campo delle comunicazioni elettroniche, include le comunicazioni a banda larga senza fili e l'Internet degli oggetti (IoT), trasporti, energia e le comunicazioni audiovisive. V. COM(2016) 587 final, 14 settembre 2016, Connettività per un mercato unico digitale competitivo: verso una società dei Gigabit europea. La Commissione ha evidenziato che la disponibilità di un idoneo quantitativo di spettro radio rappresenta uno dei presupposti essenziali per la fornitura e diffusione dei servizi *wireless* a banda larga e ultra-larga, insieme ad adeguati *standard* a garanzia di una comunicazione efficiente tra i vari componenti digitali.

uno dei presupposti essenziali per la fornitura e diffusione dei servizi *wireless* a banda larga e ultra-larga[43].

La Decisione (UE) 2017/899 del Parlamento europeo e del Consiglio prevede che entro il 30 giugno 2020 gli Stati membri autorizzino l'uso della banda di frequenza 694-790 MHz ("dei 700 MHz"). Questo spazio rappresenta il "dividendo digitale" lasciato libero dalle attività di radiodiffusione a favore dei servizi mobili di trasmissione voce e dati[44]. Al momento della concessione dei diritti d'uso, gli Stati membri autorizzano il trasferimento o l'affitto di tali diritti secondo procedure aperte e trasparenti e nel rispetto del diritto dell'Ue (art. 2). Inoltre, nell'autorizzare l'uso della banda o nel modificare i relativi diritti d'uso esistenti, essi dovranno tenere conto della necessità di conseguire specifici obiettivi di velocità e di qualità, tra cui la copertura nelle zone prioritarie nazionali predeterminate e nei principali assi di trasporto terrestre. A tal fine è prevista la possibilità di imporre condizioni ai diritti d'uso (art. 3)[45]. La decisione prevede poi la possibilità per gli Stati membri di garantire una forma di compensazione per il costo diretto della migrazione o della riassegnazione dell'uso dello spettro, soprattutto per quello a carico degli utenti finali (articolo 6). Il Codice contiene disposizioni volte ad accelerare e coordinare le procedure di assegnazione dello spettro radio per i servizi e le reti di comunicazione elettronica. Le nuove regole mirano inoltre ad armonizzare alcuni aspetti chiave dei modelli di licenza e dei regimi autorizzatori, compresa la durata minima delle licenze dei diritti d'uso individuali (almeno 15 anni), a far fronte ai problemi derivanti dalle interferenze (nazionali o transfrontaliere) dannose e a favorire, quando possibile, l'utilizzo condiviso, il trasferimento e l'affitto dello spettro sulla base del principio '*use it or lose it'*.

Il Codice ha stabilito che gli Stati membri devono consentire l'uso di almeno 1 GHz della banda di frequenze 26 GHz entro il 31 dicembre 2020, al fine di agevolare la diffusione del 5G[46]. Inoltre, la Conferenza mondiale delle radiocomunicazioni del 2019

[43]La direttiva 2014/61/UE recante misure volte a ridurre i costi dell'installazione di reti di comunicazione elettronica ad alta velocità ("direttiva sulla riduzione dei costi della banda larga", di seguito "la direttiva") mira a facilitare e incentivare la diffusione di reti di comunicazione elettronica ad alta velocità abbattendo i costi tramite un insieme di misure armonizzate. V anche COM(2018) 492 final 27 giugno 2018, sull'attuazione della direttiva 2014/61/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, recante misure volte a ridurre i costi dell'installazione di reti di comunicazione elettronica ad alta velocità.

[44] G. CAGGIANO, *La riforma del regime delle radiofrequenze nel quadro delle comunicazioni elettroniche*, in *Studi sull'integrazione europea*, 2010, p. 79 ss.

[45] Art. 54 della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche.

[46] Per il 5G La comunicazione della Commissione "Il 5G per l'Europa: un piano d'azione" ("piano d'azione per il 5G") definisce un approccio coordinato dell'Unione per la diffusione dei servizi 5G a partire dal 2020. Il piano d'azione per il 5G sollecita l'individuazione di bande di frequenza "pioniere" per il lancio dei servizi 5G da parte della Commissione in cooperazione con gli Stati membri, tenendo conto del parere del gruppo "Politica dello spettro radio" (RSPG). Nelle bande di frequenza 24,25-27,5 GHz, 37-43,5 GHz, 45,5-47 GHz, 47,2-48,2 e 66-71 GHz. In totale, la Conferenza ha identificato 17,25 GHz di spettro per IMT, rispetto a 1,9 GHz di larghezza di banda disponibile prima del WRC-19. Di questo numero, 14,75 GHz di spettro sono stati

(WRC-19) ha identificato ulteriori bande di frequenza armonizzate a livello globale (onde millimetriche) per le telecomunicazioni mobili internazionali (IMT), tra cui IMT-2020 (altrimenti noto come 5G mobile), facilitando diversi scenari di utilizzo per una banda larga mobile potenziata, enormi comunicazioni di tipo macchina e ultra-comunicazioni affidabili e a bassa latenza[47].

7. Nella politica culturale dell'Unione rientra la creazione artistica e letteraria, ivi compreso l'audiovisivo (art. 167 TFUE). Gli obiettivi dell'azione dell'Unione riguardano l'armonizzazione delle legislazioni nazionali nella prospettiva della circolazione nel mercato interno dei prodotti culturali, rafforzando al contempo la posizione di produttori, autori ed esecutori europei e, complessivamente, l'industria culturale europea. A partire dal Trattato di Amsterdam, l'Unione ha l'obbligo di tenere conto degli aspetti culturali nell'azione che svolge anche nell'ambito di altre disposizioni dei trattati sulla base della clausola di *main streaming* (art. 167, par. 6, TFUE).

La regolamentazione adottata dall'Unione negli ultimi anni riconosce maggiori possibilità di scelta e migliore accesso ai contenuti *online* transfrontalieri; norme modernizzate sul diritto d'autore, con effetti per l'istruzione, la ricerca, il patrimonio culturale e l'inclusione delle persone con disabilità; condizioni più eque e sostenibili per i creatori, le industrie creative e la stampa[48].

La territorialità dei diritti deriva dalla tendenza storica dei titolari dei diritti alla concessione di esclusive su base territoriale con la conseguente frammentazione nazionale del sistema di gestione collettiva dei diritti. Il sistema crea difficoltà ai gestori dei nuovi media *online* nell'ottenimento delle autorizzazioni/licenze[49].

Per i diritti d'autore o diritti connessi non si è consolidato il principio della legge del paese d'origine, la cui prima applicazione risale alla direttiva cavo/satellite 93/83[50]. Nella

armonizzati in tutto il mondo, raggiungendo l'85% dell'armonizzazione globale. Le prime implementazioni commerciali su vasta scala per il 5G sono attese dopo l'entrata in vigore delle specifiche IMT-2020.

[47] Regolamento (UE) 2019/1150 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online (a decorrere dal 12 luglio 2020). Per un commento, v. M. INGLESE, *La proposta di regolamento che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online: tanto tuonò che piovve*, in *Studi sull'integrazione europea*, 2019, p. 463 ss.

[48] I consumatori si aspettano di accedere a contenuti mediali mentre si spostano e attraversano le frontiere nel mercato unico. Le tecnologie digitali hanno cambiato il modo in cui la musica, i film, la televisione, la radio, i libri e la stampa vengono prodotti, distribuiti e resi accessibili al pubblico tramite nuovi servizi *online*, quali la musica *in streaming*, le piattaforme di video *on demand,* la distribuzione di *e-book* e gli aggregatori di notizie.

[49] COM(2015) 626 final, 9 dicembre 2015, Verso un quadro normativo moderno e più europeo sul diritto d'autore.

[50] Direttiva 93/83/CEE del Consiglio, del 27 settembre 1993, per il coordinamento di alcune norme in materia di diritto d'autore e diritti connessi applicabili alla radiodiffusione via satellite e alla ritrasmissione via cavo. Vi si stabilisce che "la comunicazione al pubblico via satellite si configura unicamente nello Stato Membro in cui, sotto il controllo e la responsabilità

direttiva sui servizi di media audiovisivi[51], il principio del paese d'origine non si riferisce ai diritti d'autore o ai diritti connessi, relativi alle comunicazioni al pubblico, ma riguarda la tutela dei minori e dei consumatori, in materia di pubblicità e sponsorizzazioni e di promozione delle opere europee. Rispetto all'ambito di applicazione del divieto di blocchi geografici (*geo-blocking*) resta escluso il diritto di autore, con conseguente legittimità della pratica dei professionisti di applicare diverse condizioni generali qualora siano coinvolte opere tutelate dal diritto d'autore in assenza dei necessari diritti per gli Stati interessati[52].

Alla legge del Paese di origine si riferiscono le misure sulla portabilità dei contenuti *online* e sui servizi *online* accessori delle emittenti e ai diritti sulla ritrasmissione (*simulcasting* e *catch-up* TV). Tali regole costituiscono limitate eccezioni al principio di territorialità del diritto d'autore e dei diritti connessi.

Nel regolamento di portabilità transfrontaliera dei contenuti *online*[53], ai consumatori è stato riconosciuto il diritto di utilizzare i propri abbonamenti *online* di film, musica, libri elettronici (*e-book*) quando si trovano al di fuori del paese di origine, ad esempio per vacanze o viaggi di lavoro[54]. La Commissione afferma che non intende sovvertire il principio di territorialità del diritto d'autore ma introdurre una *fictio iuris* in base alla quale l'autorizzazione, acquisita per la comunicazione di un contenuto via Internet agli abbonati residenti in uno Stato Membro, ne consente anche la comunicazione ai medesimi temporaneamente presenti in altro Stato Membro. La portabilità è configurata come un diritto dei consumatori e non come una tecnica di semplificazione nell'acquisizione dei diritti da parte dei distributori.

Anche nei servizi ancillari di trasmissione *online* (*simulcast* o *catch-up*)[55] si evoca il principio in parola. Non riguarda però le opere protette dal diritto d'autore ma soltanto servizi giornalistici e produzioni interne. Tuttavia, il legislatore introduce un meccanismo che consente all'emittente di acquisire più facilmente i diritti per questa forma accessoria di ritrasmissione *online*.

---

dell'organismo di radiodiffusione, i segnali portatori di programmi sono inseriti in una sequenza ininterrotta di comunicazione diretta al satellite e poi a terra".

[51] Direttiva 2010/13/UE del Parlamento europeo e del Consiglio, del 10 marzo 2010, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi.

[52] Cfr. art. 4, par. 1, lett. b) regolamento 2018/302.

[53] Regolamento (UE) 2017/1128 del 14 giugno 2017, relativo alla portabilità transfrontaliera di servizi di contenuti online nel mercato interno. V. anche COM(2015) 627 che garantisce la portabilità transfrontaliera dei servizi di contenuti *online* nel mercato interno.

[54] COM(2015) 627 final, Proposta di Regolamento del Parlamento Europeo e del Consiglio che garantisce la portabilità transfrontaliera dei servizi di contenuti online nel mercato interno.

[55] In riferimento ai servizi come Sky Go o Video Mediaset o La7 e non alle piattaforme per il video-on-demand come Infinity o Now TV o Netflix. Il modello si riferisce alla possibilità di ritrasmettere via Internet quanto già trasmesso sul satellite o sul digitale terrestre. G. MORBIDELLI, *Strumenti di enforcement del diritto d'autore online nella normativa europea*, in AA.VV., *Liber Amicorum in onore di Antonio Tizzano: De la Cour CECA à la Cour de l'Union: le long parcour de la justice européenne*, Torino, 2018, p. 640 ss.

8. Il Regolamento (UE) 2018/302 reca misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno[56]. Per *geo-blocking* si intendono pratiche messe in atto da venditori *online* per imporre limitazioni alle transazioni transfrontaliere digitali, comportando eventualmente il re-indirizzamento automatico degli utenti a siti *web* di fornitori con sede nello Stato membro dei clienti[57].

Si tratta dell'attuazione al principio generale del diritto UE di non discriminazione (anche indiretta) sulla base della nazionalità definito dall'art. 18 TFUE e dall'art. 21, par. 2 della Carta dei diritti fondamentali, nonché delle disposizioni specifiche del Trattato a tutela del mercato interno.

Tuttavia, i blocchi geografici sono vietati nella misura in cui non siano oggettivamente giustificati ai sensi del diritto dell'Unione, vale a dire quelle disparità di trattamento che non possono essere ammesse alla luce dei "criteri oggettivi" (direttiva servizi 2006/123/CE)[58].

Quanto all'accesso alle interfacce *online*, il professionista non può bloccare l'accesso al proprio sito *web*, né reindirizzare ad una versione diversa da quella richiesta senza il previo consenso del cliente. E anche a fronte dell'assenso, la versione originale visitata deve rimanere consultabile. Tuttavia, il rispetto di taluni requisiti previsti dal diritto dell'Unione o da leggi nazionali conformi (applicabili al caso di specie) può legittimare blocchi, limitazioni o un mero re-indirizzamento. In tali circostanze, il professionista ha l'obbligo di fornire ai clienti una "spiegazione chiara e specifica"[59] nella lingua dell'interfaccia *online* cui il cliente desiderava accedere.

In merito alla disciplina di accesso ai beni e ai servizi, la direttiva servizi in parola ribadisce il divieto di praticare condizioni generali di accesso diverse per motivi di nazionalità, residenza, stabilimento in talune ipotesi quali la vendita di beni senza consegna al di fuori della zona servita dal professionista o quella di servizi prestati tramite

[56] Regolamento (UE) 2018/302 del Parlamento europeo e del Consiglio, del 28 febbraio 2018, recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno e che modifica i regolamenti (CE) n. 2006/2004 e (UE) 2017/2394 e la direttiva 2009/22/CE.

[57] C. PESCE, *Blocchi geografici ingiustificati. Unjustified Geo-blocking*, in *I Post di AISDUE*, 5 aprile 2019.

[58] Direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno, art. 20, par. 2. La direttiva del 2006 si applica laddove la disciplina del *geo-blocking* non contenga disposizioni più specifiche intese come insieme di regole chiare, uniformi ed efficaci su aspetti particolari (art. 1, paragrafi 1 e 7 regolamento 2018/302). sentenza della Corte di giustizia del 19 dicembre 2018, causa C-572/17, *Syed*; sentenza della Corte di giustizia (Grande Sezione) del 13 novembre 2018, causa C-310/17, *Levola Hengelo.*

[59] Cfr. art. 3, par. 3, seconda frase regolamento 2018/302.

mezzi elettronici o erogati in un luogo fisico specifico[60]. In tal caso, la protezione dei consumatori opera appieno o in misura maggiore rispetto a quanto visto per l'accesso alle interfacce *online*, atteso che, in tali circostanze, blocchi geografici o disparità di trattamento su base geografica sono ammessi solo in situazioni eccezionali.

I professionisti hanno, in linea di principio, la facoltà di decidere quali modalità di pagamento accettare[61]. Tuttavia, una volta effettuata la scelta, non è consentito opporre ai clienti UE rifiuti nelle transazioni o applicare loro condizioni di corresponsione diverse per i motivi geografici detti.

Spetta, inoltre, alla normativa nazionale definire i poteri o i mezzi di ricorso giurisdizionali e/o amministrativi esperibili da parte di chi lamenta una violazione dei propri diritti nel contesto delle operazioni commerciali *online* di carattere transfrontaliero[62]. Di particolare rilevanza è l'articolo 8 del regolamento 2018/302, ai sensi del quale ogni Stato membro designa uno o più organismi chiamati a fornire assistenza ai consumatori in caso di contrasti con un professionista derivante dall'applicazione del regolamento.

9. Secondo la direttiva 2019/790 sul diritto d'autore[63], la responsabilità editoriale degli ISP che diffondono contenuti o altri materiali protetti dal diritto d'autore caricati dai loro utenti (servizi di *streaming* audio e video *online*) deriva dalla comunicazione al pubblico.

Prima dell'adozione della strategia sul mercato digitale unico, la direttiva 2014/26/UE ha introdotto la gestione collettiva dei diritti d'autore e dei diritti connessi e la concessione di licenze multi-territoriali per i diritti su opere musicali per l'uso *online*; ha stabilito obblighi di trasparenza e di informazione, nonché una serie di prescrizioni circa le modalità di esercizio dell'attività di gestione collettiva in capo a tutti i soggetti che svolgono attività di intermediazione al riguardo. Questi requisiti sono tuttavia differenziati a seconda che si tratti di un "organismo di gestione collettiva" ovvero un'"entità di gestione indipendente" (vale a dire, un intermediario non controllato dai titolari dei diritti o dai relativi rappresentanti). Nel secondo caso, si applicano solo un numero limitato di obblighi di trasparenza, informazione e sulle modalità di esercizio della gestione collettiva.

Per quanto riguarda le misure per la concessione di licenze collettive con effetto esteso, in particolare gli Stati possono prevedere che laddove un organismo di gestione collettiva stipuli, in conformità ai mandati ricevuti dai titolari dei diritti, un accordo di licenza per lo sfruttamento di opere o altri materiali, tale accordo possa essere esteso

[60] Cfr. art. 4 regolamento 2018/302. Si tratta di servizi di *cloud computing*, di archiviazione di dati o di *hosting* di siti *Internet*.
[61] Cfr. art. 5 regolamento 2018/302.
[62] Procedimenti amministrativi o giudiziari; azioni di danni; sanzioni amministrative o penali etc.
[63] Direttiva 2019/790, del Parlamento europeo e del Consiglio del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale. M. ZANCAN, *La nuova direttiva sul diritto d'autore e sui diritti connessi nel mercato unico digitale***,** in *MediaLaws*, 2/2019, p. 338 ss.

anche ai titolari di diritti che non abbiano autorizzato il predetto organismo a rappresentarli; meccanismo applicabile a settori ben definiti, dove per un insieme di fattori l'ottenimento delle autorizzazioni individuali da parte degli interessati è oneroso e poco pratico; sono previste misure a salvaguardia dei titolari dei diritti (art. 12) e la creazione di un organismo imparziale o di mediatori per l'assistenza alla negoziazione di accordi di licenza per opere audiovisive su servizi di video su richiesta, di cui possano avvalersi le parti che incontrano difficoltà a concludere tali accordi (art. 13).

Eccezioni e limitazioni al diritto d'autore correlate all'uso digitale sono previste a scopi educativi, scientifici e di conservazione del patrimonio culturale; è riconosciuto un diritto degli editori di giornali alla remunerazione per l'utilizzo *online* delle loro pubblicazioni; nonché un obbligo per le piattaforme digitali che memorizzano e danno accesso a grandi quantità di opere e materiali caricati dagli utenti, di adottare misure adeguate e proporzionate, volte a garantire il funzionamento degli accordi conclusi con i titolari di diritti. Un importante elemento di novità, il quale ha suscitato un acceso dibattito, è quello dell'introduzione di un diritto connesso al diritto d'autore a favore degli editori, per l'utilizzo in ambito digitale, mediante riproduzione e messa a disposizione del pubblico, di pubblicazioni di carattere giornalistico da parte di prestatori di servizi della società dell'informazione (art. 15); riguarda anche le riproduzioni parziali delle pubblicazioni di carattere giornalistico, con una durata di 2 anni.

L'altro pilastro della direttiva concerne l'obbligo per i prestatori di servizi di condivisione di contenuti *online*, di ottenere l'autorizzazione dei titolari, ad esempio attraverso accordi di licenza, quando concedono l'accesso al pubblico a opere o altri materiali protetti caricati dai loro utenti, attività che la direttiva definisce quali atti di comunicazione al pubblico, così riconducendoli alla fascia di facoltà esclusive spettanti all'autore (art. 17). L'autorizzazione include anche gli atti compiuti dagli utenti, che non agiscano su base commerciale o la cui attività non generi ricavi significativi[64].

[64] Ricorso proposto il 24 maggio 2019, *Repubblica di Polonia c. Parlamento europeo e Consiglio dell'Unione europea*, causa C-401/19, per annullare l'art. 17, par. 4, lett. b), e l'art. 17, par. 4, lett. c), in fine (ossia, nella parte che include le parole: "e aver compiuto i massimi sforzi per impedirne il caricamento in futuro conformemente alla lettera b)") della direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE. Avverso le disposizioni impugnate della direttiva 2019/790 la Repubblica di Polonia deduce il motivo relativo alla violazione del diritto alla libertà di espressione e di informazione, garantito dall'articolo 11 della Carta dei diritti fondamentali dell'Unione europea. La Repubblica di Polonia sostiene, in particolare, che l'assoggettamento dei prestatori di servizi di condivisione di contenuti *online* all'obbligo di compiere i massimi sforzi per assicurare che non siano disponibili opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti (articolo 17, paragrafo 4, lettera b), nonché l'imposizione a carico dei prestatori di servizi di condivisione di contenuti *online* dell'obbligo di compiere i massimi sforzi per impedirne il caricamento in futuro delle opere o di altri materiali protetti, che sono stati oggetto di una segnalazione sufficientemente motivata da parte dei titolari dei diritti (*ivi*, lettera c), in fine), rende necessario, per non incorrere in responsabilità, che i prestatori effettuino una verifica automatica preventiva (filtraggio) dei contenuti condivisi online dagli utenti e, di conseguenza, che introducano i meccanismi di controllo preventivo. Un siffatto meccanismo pregiudica

Alcune tipologie di piattaforme come le "architetture di interazione" in cui gli utenti producono e condividono materiale (*Youtube*) cominciano a ricevere così una regolamentazione sul rispetto del diritto d'autore. La comunicazione è legittima soltanto quando il gestore della piattaforma/prestatore del servizio ottenga un'autorizzazione dai titolari dei diritti mediante la conclusione di un accordo di licenza o altro strumento negoziale di autorizzazione alla diffusione dell'opera[65]. Pertanto, uno dei principali obiettivi della direttiva è quello di assicurare per gli autori e gli artisti (interpreti o esecutori) un'adeguata remunerazione che sia proporzionata al valore economico effettivo o potenziale dei diritti concessi in licenza o trasferiti. In tema di remunerazione, la direttiva specifica che gli accordi potrebbero anche giungere alla previsione di un pagamento forfettario delle licenze, ma ciò non dovrebbe rappresentare la regola, tenuto conto delle specificità di ciascun settore. Al fine di facilitare la conclusione di questi accordi, la direttiva incarica gli Stati membri di offrire la possibilità alle parti di avvalersi dell'assistenza di un mediatore o di un organismo imparziale.

Pur ribadendosi l'assenza di un obbligo generale di sorveglianza a carico dei prestatori di servizi di condivisione *online* di contenuti, ne rafforza ora obblighi e responsabilità, sia pure in un'ottica proporzionale alla salvaguardia di *start-up* e di piccole e medie imprese, nonché dell'utente "non commerciale". In assenza di autorizzazione, il prestatore di servizi di condivisione di contenuti *online* è responsabile per gli atti non autorizzati di comunicazione al pubblico di opere e altri materiali protetti dal diritto d'autore, salvo che non dimostri: (i) di avere posto in essere i massimi sforzi per ottenere la predetta autorizzazione; (ii) di avere compiuto secondo elevati *standard* di diligenza professionale di settore, i massimi sforzi per assicurare che non siano disponibili opere e materiali specifici per i quali abbia ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti; e, in ogni caso (iii) avendo ricevuta una segnalazione sufficientemente motivata dai titolari dei diritti, abbia provveduto tempestivamente a disabilitare l'accesso o rimuovere dal proprio sito web i contenuti protetti, compiendo il massimo sforzo per impedirne il caricamento in futuro. La valutazione dell'assolvimento dei predetti obblighi gravanti sul prestatore di servizi deve avvenire, alla stregua del principio di proporzionalità, considerando *inter alia* pubblico, dimensione del servizio, tipo di opere caricate, disponibilità e costo di strumenti adeguati ed efficaci per i prestatori di servizi. È prevista una significativa limitazione degli obblighi nei confronti di *start up* e di piccole e medie imprese, tenuto conto del tempo in cui esse operano, del loro fatturato e del numero di visualizzazioni individuali, con un sistema crescente di presidi in relazione ai diversi parametri.

Sotto il profilo degli utenti, la direttiva prevede che essi possano avvalersi, rispetto ai contenuti caricati e messi a disposizione, delle eccezioni di citazione, critica, rassegna,

l'essenza del diritto alla libertà di espressione e di informazione e non soddisfa i requisiti di proporzionalità e di necessità di limitazioni di tale diritto.

[65] L. AMMANNATI, *Verso un diritto delle piattaforme digitali*? in *federalismi.it*, 2019/7, p. 3 ss.; A. CANEPA, *Le piattaforme fra nuove dinamiche di mercato e ricerca di strumenti regolatori efficaci,* in *Rivista della Regolazione dei mercati*, 2018/2, p. 181 ss.

nonché che possano essere utilizzati a scopo di caricatura, parodia o *pastiche*, salvaguardando in generale gli utilizzi legittimi previsti dal diritto UE. Sono altresì previsti meccanismi di reclamo e di ricorso celere per il caso di controversie relative alla rimozione di contenuti o disabilitazione all'accesso, meccanismi di ricorso stragiudiziale, nonché oneri informativi dei prestatori di servizi di condivisione nei confronti dei loro utenti.

La direttiva afferma il principio secondo il quale gli autori e gli artisti (interpreti o esecutori) che concedono in licenza o trasferiscano i diritti esclusivi per lo sfruttamento delle loro opere o materiali abbiano il diritto di ricevere una remunerazione adeguata e proporzionata, lasciando agli Stati membri la scelta dei meccanismi per darvi attuazione, tenuto conto del principio di libertà contrattuale e del bilanciamento di diritti e interessi coinvolti (art. 18). In tale ambito, prevede: un obbligo di trasparenza, proporzionato ed effettivo, avente ad oggetto informazioni periodiche, complete, pertinenti ed aggiornate sullo sfruttamento delle opere concesse in licenza, in particolare su forme di sfruttamento, proventi generati e remunerazione dovuta (art. 19); un meccanismo di adeguamento contrattuale, in mancanza di un accordo di contrattazione collettiva che preveda un dispositivo comparabile, in favore di autori ed artisti, i quali possono rivendicare una remunerazione ulteriore adeguata ed equa nell'ipotesi in cui quella originariamente concordata si sia rivelata sproporzionatamente bassa rispetto ai proventi originati in un secondo tempo rispetto alle loro opere o esecuzioni (art. 20); una procedura alternativa di risoluzione delle controversie (art. 21) ed infine il diritto degli autori ed artisti (interpreti o esecutori) di revoca (che può essere subordinato a determinati parametri temporali) della licenza o del trasferimento esclusivi dei propri diritti sull'opera o altri materiali protetti in caso di mancato sfruttamento degli stessi (art. 22).

La direttiva introduce un nuovo "diritto connesso" per gli editori, analogo a quello per i produttori di film, i produttori discografici e le emittenti. La direttiva istituisce nuovi meccanismi di negoziazione per la conclusione di accordi di licenza per lo sfruttamento dei contenuti protetti sulle piattaforme *online* che, invece di dover negoziare individualmente, saranno in grado di ottenere le licenze tramite organismi di gestione collettiva rappresentative dei titolari dei diritti. Il titolare dei diritti ha la facoltà sia di scegliere un organismo di gestione collettiva situato in un paese diverso da quello della propria nazionalità o in cui risiede; sia di affidare la gestione dei propri diritti a entità di gestione indipendenti; sia soggetti di gestione di licenze multi-territoriali per la musica *online*. Il meccanismo innovativo dovrebbe comprendere piattaforme per la concessione di licenze.

In relazione alla nozione di "comunicazione al pubblico", la Corte di giustizia ha più volte ribadito che va interpretata alla luce delle convenzioni internazionali in materia, associando due elementi cumulativi: un atto di comunicazione di un'opera protetta e un pubblico a cui quell'opera è comunicata[66]. Secondo la Corte, il concetto di

[66] Sentenze del 16 marzo 2017, causa C-138/16, *Zurs.net*; del 7 agosto 2018, causa C-161/2017, *Renckhoff*.

"comunicazione al pubblico" comprende quelle piattaforme che, tramite la loro attività, creano un "pubblico nuovo" a contenuti già esistenti *online* in violazione del diritto d'autore[67].

La Corte di giustizia fonda il proprio ragionamento soprattutto sul ruolo dell'utente che realizza la comunicazione e sul carattere intenzionale del suo intervento. Si ha comunicazione quando l'utente interviene, con piena cognizione delle conseguenze del proprio comportamento, per consentire ai propri clienti l'accesso ad un'opera protetta[68]. Gli amministratori di piattaforme internet di condivisione non sono meri fornitori di attrezzature fisiche per la comunicazione[69] se propongono un motore di ricerca delle opere e un relativo indice di classificazione. Al contrario, il loro ruolo attivo li rende autori di una comunicazione al pubblico di opere protette, comunicazione che i titolari dei relativi diritti possono bloccare se non autorizzata. Essi cessano di fare attività di *mere conduit* tramite trasporto dei dati in modo asettico e indifferente, perché l'attività di indicizzazione ha un valore aggiunto determinante, consentendo di individuare i file suscettibili di trasferimento e, attraverso i protocolli, di trasferirli sul computer.

Nella sentenza *VSAT*, la Corte ricomprende ogni comunicazione al pubblico, inclusa quella realizzata tramite l'intervento attivo dell'operatore che mette a disposizione opere protette per la registrazione su *cloud* di emissioni tv. Anche in questo caso, il titolare del diritto d'autore o del diritto connesso dunque è libero di decidere se autorizzare o vietare anche tale utilizzazione della sua opera[70].

Nella sentenza *Telekabel*[71], la Corte statuisce che ad un fornitore di accesso alla Rete può essere ordinato di bloccare l'accesso dei suoi abbonati ad un sito che viola il diritto d'autore, a condizione che l'ingiunzione e la sua esecuzione rispettino un giusto equilibrio tra i diritti fondamentali interessati. Ciò si verifica se le misure in discussione non privino inutilmente gli utenti di Internet della possibilità di accedere in modo lecito alle informazioni disponibili, anche se, al contempo, hanno l'effetto di impedire o, almeno, di rendere difficilmente realizzabili le consultazioni non autorizzate di materiali protetti messi a disposizione in violazione del diritto di proprietà intellettuale.

[67] Secondo la sentenza 14 giugno 2017, causa C-610/15, *Stichting Brein ("Pirate Bay")*, ECLI:EU:C:2017:456. V. anche, in precedenza, sentenza 26 aprile 2017, causa C-527/15, *Stichting Brein (Filmspeler)*, ECLI:EU:C:2017:300.
[68] *Phonographic Performance (Ireland)* e *Pirate Bay*.
[69] Esclusi dal considerando 7 dal campo di applicazione della direttiva 2001/29/CE del Parlamento europeo e del Consiglio del 22 maggio 2001 sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione.
[70] Sentenza 29 novembre 2017, causa C-265/16, *VCAST Limited*, ECLI:EU:C:2017:913.
[71] Sentenza del 27 marzo 2014, causa C-314/12, *UPC Telekabel*, ECLI:EU:C:2014:192.

In materia di diritto d'autore, la Corte di giustizia ha fornito anche altre importanti indicazioni nelle sentenze *Promusicae e Bonnier Audio* [72], *Sabam* e *Netlog*[73], *Svensson*[74].

10. La dimensione europea del mercato audiovisivo si è espansa a causa della crescita dei servizi *online*, mentre le trasmissioni televisive diventano sempre più transnazionali (quasi un terzo trasmette verso un altro Stato membro). Nel 2010, la direttiva di servizi di media audiovisivi è stata estesa ai servizi audiovisivi per includere servizi *video-on-demand* e canali Internet (servizi non-lineari)[75]. Il principio di base è quello secondo cui ciascuno Stato membro deve imporre determinati requisiti minimi sui servizi di media audiovisivi sottoposti alla sua giurisdizione ("principio del paese di origine"). Per effetto di questo controllo originario, un servizio può essere trasmesso in altri Stati membri senza ulteriori controlli.

La direttiva 2018/1808 sui servizi media[76] tiene conto della affermazione di nuovi operatori, fra cui le piattaforme *online* per la condivisione di video che anche se privi di responsabilità editoriale sui contenuti, li organizzano in vari modi e, di fatto, si pongono in concorrenza con i fornitori di servizi media tradizionali. Pertanto, alcune misure di regolamentazione tipiche dei media audiovisivi vengono estese anche alle piattaforme *online*[77]. Si tratta di un intervento molto rilevante perché si tiene conto, sia pure in modo

[72] Sentenze del 29 gennaio 2008, causa C-275/06, *Promusicae*, ECLI:EU:C:2008:54; del 19 aprile 2012, causa C-461/10, *Bonnier Audio*, ECLI:EU:C:2012:219. Nell'ambito degli illeciti commessi tramite internet, dopo la soluzione negativa nel caso Promusicae, la seconda è più favorevole ai titolari dei diritti, dal momento che la Corte valuta prevalenti gli interessi dei titolari dei diritti rispetto alla protezione dei dati personali degli autori delle violazioni.

[73] Sentenze del 24 novembre 2011, causa C-70/10, *Scarlet*, ECLI:EU:C:2011:771 e del 16 febbraio 2012, causa C-360/10, *Sabam,* ECLI:EU:C:2012:85.

[74] Sentenza del 13 febbraio 2014, causa C-466/12, *Svensson*, ECLI:EU:C:2014:76. Questa sentenza rende più chiari i confini della "comunicazione al pubblico" di opere protette in Internet tramite la tecnica del *linking*. Salvo il caso in cui le opere siano già liberamente accessibili in rete, qualsiasi altra messa a disposizione di esse al pubblico deve essere autorizzata dai titolari dei diritti.

[75] Direttiva 2010/13/UE del Parlamento europeo e del Consiglio, del 10 marzo 2010, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi.

[76] Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio del 14 novembre 2018 recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi, v. R. MASTROIANNI, *La determinazione del country of origin ed il principio del mutuo riconoscimento nel nuovo testo della direttiva sui servizi di media audiovisivi*, in *Temi e questioni di diritto dell'Unione europea*, in *Scritti offerti a Claudia Morviducci,* p. 259 ss.

[77] In particolare, nel Considerando 5) della direttiva, si stabilisce che: "i servizi di *social media* o *social network* dovrebbero essere sottoposti a regolamentazione se la fornitura di programmi e di video generati dagli utenti costituisce una loro funzionalità essenziale. Inoltre, benché tali piattaforme online non detengano esattamente una responsabilità editoriale sui contenuti veicolati, tuttavia, in genere, determinano l'organizzazione di tali contenuti, ossia programmi, video generati dagli utenti e comunicazioni commerciali audiovisive, anche in modo automatizzato o con algoritmi. Pertanto, in base al riconoscimento che tali piattaforme

limitato, dell'avvenuta ibridazione di alcune tipologie di piattaforma *online* con i "servizi di media audiovisivi", ampliando il campo di applicazione della direttiva. La conseguenza è quella di imporre obblighi di comportamento finalizzati sia a un più corretto equilibrio nel rapporto con i mezzi di diffusione tradizionali, sia a proteggere gli utenti, in particolare i minori, da contenuti illegali e comunque pregiudizievoli del loro sviluppo.

Secondo l'art. 28-*ter* della nuova direttiva, tali piattaforme dovranno adottare misure per la tutela dei minori, contro la violenza, l'odio e contenuti la cui diffusione costituisce un'attività che rappresenta un reato. In particolare, la direttiva stabilisce che l'adeguatezza delle misure tecnico/contrattuali, adottate secondo schemi di auto- o co-regolamentazione, deve in ultima analisi essere valutata dalle ANR. È possibile per gli Stati membri adottare misure più restrittive o dettagliate, a condizione di rispettare il diritto dell'Unione (*ivi*, par. 6), ed in particolare le regole sulla limitazione di responsabilità codificate nella direttiva e-Commerce[78] (articoli 12-15), e direttiva 2011/93[79] sulla pedo-pornografia (art. 25).

Quanto ai criteri di definizione dello Stato di giurisdizione, due procedure sono intese ad aumentare il livello di trasparenza e conoscibilità dei dati relativi allo stabilimento delle emittenti. Il primo richiede agli Stati membri di assicurare che i fornitori di servizi di media informino le autorità o gli organismi nazionali di regolamentazione competenti di qualsiasi modifica rielevante; il secondo richiede agli Stati membri di creare un elenco dei fornitori di servizi di media audiovisivi, aggiungendo i criteri sui quali si fonda la loro giurisdizione (art. 2, paragrafi 5-*bis* e 5-*ter*).

Dal punto di vista generale, appare rilevante quanto stabilito sull'inclusione delle piattaforme non stabilite nel territorio di uno Stato membro ai fini dell'applicazione della direttiva, utilizzando un sistema a cascata che tende ad estendere il campo di applicazione delle nuove regole e coinvolge le società madri, controllate o facenti parte di un gruppo, se stabilite nel territorio di uno Stato membro. Se più società controllate sono stabilite in diversi Stati membri, la piattaforma si considera stabilita nello Stato in cui l'attività è iniziata. Infine, anche in questo caso agli Stati membri viene richiesto di creare una lista di piattaforme che ritengono stabilite nel loro territorio in base ai criteri e attribuisce alla Commissione il compito di dirimere eventuali conflitti di giurisdizione tra Stati membri.

Un altro aspetto rilevante della direttiva è l'obbligo che le emittenti europee riservino quote di trasmissione alle "opere europee". La direttiva di modifica amplia il campo di applicazione della direttiva includendo le piattaforme per la condivisione di video generati dagli utenti (ad es. You-Tube), rafforzando gli obblighi per i servizi a richiesta.

promuovono contenuti di informazione e intrattenimento come "funzionalità essenziale" e che sono predisposte per "organizzare" la visione di contenuti, esse dovrebbero essere tenute ad adottare le misure appropriate per tutelare le varie categorie di consumatori".

[78] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»).

[79] Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio.

Per questi ultimi, la direttiva introduce la facoltà per gli Stati membri di imporre obblighi finanziari non solo ai soggetti sottoposti alla propria giurisdizione, ma anche a quelli stabiliti in un altro Stato membro che si rivolgono al proprio pubblico nazionale[80].

11. La nuova direttiva 2019/789 sugli organismi di diffusione radiotelevisiva e ritrasmissioni di programmi televisivi e radiofonici[81] consente alle emittenti di ottenere più facilmente le autorizzazioni dei titolari dei diritti di cui hanno bisogno per trasmettere programmi online in altri Stati membri. Si tratta di programmi che le emittenti trasmettono *online* contemporaneamente alle loro trasmissioni televisive nonché ai servizi di *catch up* che desiderano mettere a disposizione *online* in altri Stati membri. Le norme rendono più facile, per gli operatori che offrono pacchetti di canali televisivi, ottenere le licenze e le autorizzazioni necessarie, invece di dover negoziare individualmente con ciascun titolare di diritti tramite organismi di gestione collettiva rappresentativi dei titolari dei diritti.

Per quanto riguarda la trasmissione e la ritrasmissione *online* dei programmi televisivi e radiofonici, le emittenti offrono sempre più tale modalità[82]. La prestazione di tali servizi si basa sempre di più su tecnologie diverse (ad esempio satellite, IPTV, digitale terrestre, reti mobili, Internet) dalla trasmissione via cavo, ai cui operatori si applicano le regole esistenti[83]. Un'emittente deve ottenere, per ciascuno Stato membro in cui i

[80] Sulla direttiva, v. G. CAGGIANO, *Paese di origine, competenza giurisdizionale e misure derogatorie della circolazione dei servizi audiovisivi*, in *Rivista dell'informazione e dell'informatica*, 2010, p. 175 ss.; R. MASTROIANNI, *La direttiva sui servizi di media audiovisivi e la sua attuazione nell'ordinamento italiano,* Torino, 2009 (II ed. 2011).
In materia di diritto d'autore e diritti vicini a tutela dei prodotti dell'ingegno e della creatività, vi sono numerosi atti di armonizzazione delle legislazioni degli Stati membri, anche in attuazione di trattati internazionali. La direttiva 2001/29 sull'armonizzazione di taluni aspetti dei diritti d'autore e connessi nella società dell'informazione ha dato, tra l'altro, applicazione ai due Trattati approvati nel 1996 dall'OMPI: il Trattato sul diritto d'autore (WCT) in linea di continuità con la Convenzione di Berna; il Trattato sulle interpretazioni, le esecuzioni e i fonogrammi (WPPT) che Ammoderna la Convenzione di Roma del 1961.
Direttiva 2014/26/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sulla gestione collettiva dei diritti d'autore e dei diritti connessi e sulla concessione di licenze multi-territoriali per i diritti su opere musicali per l'uso online nel mercato interno. La Corte di giustizia ha statuito sulla tendenziale conformità della struttura monopolistica delle società di gestione collettiva al diritto dell'Unione (v. sentenza 27 febbraio 2014, causa C-351/12, *OSA*, ECLI:EU:C:2014:110, punto 72).

[81] Direttiva (UE) 2019/789 del Parlamento europeo e del Consiglio del 17 aprile 2019 che stabilisce norme relative all'esercizio del diritto d'autore e dei diritti connessi applicabili a talune trasmissioni online degli organismi di diffusione radiotelevisiva e ritrasmissioni di programmi televisivi e radiofonici e che modifica la direttiva 93/83/CEE del Consiglio

[82] Tra i servizi inclusi vi sono la diffusione simultanea *online* di trasmissioni (*simulcasting*), che dà la possibilità di guardare e/o ascoltare programmi radiotelevisivi per un periodo di tempo determinato dopo la loro trasmissione iniziale (*catch-up*), e l'offerta di contenuti che arricchiscono, integrano o ampliano le trasmissioni (ad esempio anteprime o contenuti complementari come i "dietro le quinte").

[83] Gli operatori via cavo beneficiano già di una gestione collettiva obbligatoria ai sensi della vigente direttiva sulla trasmissione via satellite e via cavo (direttiva 93/83/CEE).

programmi saranno disponibili *online*, autorizzazioni distinte da vari titolari di diritti, per diverse categorie di opere e altri contenuti protetti.

La nuova direttiva affronta le difficoltà connesse all'acquisizione dei diritti d'autore in due modi: stabilendo il principio del "paese d'origine", in base al quale i diritti necessari per rendere disponibili alcuni programmi mediante i servizi *online* offerti dalle emittenti devono essere acquisiti unicamente per il paese in cui l'emittente ha la sua sede principale (anziché per tutti gli Stati membri in cui l'emittente intende rendere disponibili i propri programmi). Il canone corrisposto dalle emittenti ai titolari dei diritti dovrà essere proporzionato al pubblico dei programmi. Il principio del paese d'origine non si applica ai servizi di video su richiesta (VOD).

Il principio del paese d'origine si applicherà a tutti i programmi radiofonici e ad alcuni programmi televisivi, vale a dire i notiziari e i programmi di attualità, così come le produzioni interamente finanziate dagli organismi di diffusione radiotelevisiva. Il principio del paese d'origine non si applicherà invece alle produzioni televisive acquistate da terzi o commissionate dagli organismi di diffusione radiotelevisiva a produttori indipendenti. Sono escluse anche le trasmissioni televisive di eventi sportivi.

La direttiva chiarisce che, quando le emittenti trasmettono i loro segnali portatori di programmi mediante immissione diretta unicamente ai distributori[84] e questi ultimi li trasmettono al pubblico, si realizza un atto di comunicazione al pubblico, cui partecipano sia l'emittente sia i distributori e per il quale essi devono ottenere un'autorizzazione dai titolari dei diritti. Nel caso *ITV Broadcasting*, la Corte di giustizia ha stabilito, in una prima sentenza, che le emittenti televisive possono vietare la ritrasmissione via internet dei loro programmi senza l'autorizzazione da parte del loro autore. Una seconda sentenza ha dichiarato le norme britanniche incompatibili con il diritto dell'Unione, confermando la propria giurisprudenza favorevole alla massima tutela nei nuovi scenari tecnologici, soprattutto in riferimento al concetto di comunicazione al pubblico[85].

Ipotesi specifica è quella dell'immissione da un produttore di programmi che non si rivolge direttamente al pubblico ma solo ad una emittente che svolge un'attività puramente tecnica. Nella sentenza *SBS Belgium*, la Corte non esclude che in alcuni casi gli autori della trasmissione originaria siano tenuti al pagamento dei compensi a favore dei titolari dei diritti, se l'intervento dei distributori è di tipo esclusivamente tecnico[86]. La Corte ricorda che "ogni trasmissione o ritrasmissione di un'opera che utilizzi uno

[84] L'immissione diretta rappresenta un processo sempre più diffuso tra le emittenti per trasmettere programmi al pubblico. Invece di trasmettere i loro programmi direttamente al pubblico via etere o su filo, le emittenti inviano i loro programmi ai distributori, che li trasmettono al pubblico.

[85] Sentenza 7 marzo 2013, causa C-607/11, *ITV Broadcasting Ltd e al*., ECLI:EU:C:2013:147. A seguito della sentenza, i giudici britannici hanno ritenuto che non si configurasse alcuna violazione delle disposizioni normative interne sulla liceità della ritrasmissione via cavo in simultanea, limitatamente alle zone a cui le trasmissioni erano originariamente destinate. La decisione della High Court è stata impugnata dinanzi alla Court of Appeal, che ha proposto il nuovo rinvio pregiudiziale. V. sentenza 1° marzo 2017, causa C-275/15, *ITV Broadcasting Limited e a.*, ECLI:EU:C:2017:144.

[86] Sentenza del 19 novembre 2015, causa C-325/14, *SBS Belgium*.

specifico mezzo tecnico deve essere, in linea di principio, autorizzata individualmente dall'autore" e non dubita che la trasmissione in discussione costituisca un atto di comunicazione. Per i giudici, tuttavia, manca il secondo requisito della comunicazione al pubblico, ossia la presenza del pubblico stesso (i distributori, infatti, non possono essere considerati "pubblico" e i segnali trasmessi loro da SBS non sono visibili agli abbonati). Quando trasmette i segnali dei programmi ai distributori, dunque, SBS Belgium non effettua una comunicazione al pubblico di opere protette. Con una precisazione importante: se il giudice nazionale verifica che "l'intervento dei distributori costituisce soltanto un semplice mezzo tecnico", per cui essi non agiscono in modo autonomo rispetto all'organismo radio-tv, allora gli abbonati dei distributori costituiscono il pubblico della comunicazione originaria e l'organismo radio-tv dovrà pagare i compensi spettanti ai titolari dei diritti.

12. Alle piattaforme *online*, specie ai motori di ricerca e *social media* è stato riconosciuto un ruolo di controllore dei contenuti informativi. In particolare, la Corte di giustizia nella sentenza *Google Spain* ha riconosciuto una "delega di funzioni pubbliche"[87] tramite il potere di valutare e deindicizzare i dati che non corrispondono *più* all'identità personale dell'interessato (diritto all'oblio) e la rimozione dei contenuti illeciti. La Corte di giustizia ha affidato al motore di ricerca il compito di valutare le richieste di de-indicizzazione sollecitate dagli interessati[88].

Anche rispetto alla circolazione dei dati personali extra-UE, nella sentenza *Schrems*[89] la Corte ha dichiarato l'invalidità totale della decisione di adeguatezza della Commissione[90]. Il principio di base è rappresentato dall'obbligo di equivalenza della tutela negli ordinamenti degli Stati terzi e dell'Unione europea. In tale contesto, i meccanismi di tutela dei dati personali si applicano sia nei confronti di imprese operanti nel mercato unico con la sede principale extra-UE, sia nei confronti delle autorità pubbliche di Stati terzi che acquisiscono i dati "provenienti" dagli Stati membri.

Nella sentenza *Google/CNIL*[91], la Corte ha statuito che il gestore di un motore di ricerca non è tenuto a effettuare la deindicizzazione in tutte le versioni del suo motore di

[87] Ovvero l'interesse individuale alla rimozione di notizie non più corrispondenti all'identità personale dell'individuo se illecite o raccolte lecitamente ma per finalità diverse.
[88] Il principio è stato codificato dall'art. 17 del GDPR, insieme ad una deroga per: a) l'esercizio del diritto alla libertà di espressione e di informazione; b) l'adempimento di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri; c) motivi di interesse pubblico nel settore della sanità pubblica d) fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria (ivi, par.3). In argomento, v. EDPB, Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1), 2 December 2019.
[89]Sentenza della Corte (Grande Sezione) del 6 ottobre 2015, causa C-362/14, *Schrems*, ECLI:EU:C:2015:650.
[90] La circolazione dei dati personali extra-UE è soggetta al controllo tramite atti di esecuzione della Commissione ("decisioni di adeguatezza").
[91] Sentenze della Corte di giustizia del 24 settembre 2019, causa C-507/17, *Google-CNIL*, ECLI:EU:C:2019:772.

ricerca, ma solo in quelle corrispondenti a tutti gli Stati membri. Il gestore dovrebbe attuare misure di *geoblocking* che scoraggino gli utenti dall'avere accesso, a partire da uno degli Stati membri, ai *link* di cui trattasi contenuti nelle versioni extra UE di detto motore[92]. Nella sentenza *GC/CNIL*[93] la Corte ha affermato che i gestori di motori di ricerca devono esaminare, su richiesta di deindicizzazione dell'interessato, se un semplice *link* verso una pagina *web* contenente dati sensibili sia strettamente necessario per proteggere la libertà di informazione. Nella sentenza *Eva Glawischnig-Piesczekan*[94], la Corte ha stabilito che, in base alla direttiva sul commercio elettronico, un prestatore di servizi di *hosting* (Facebook) può essere richiesto di rimuovere commenti identici e a certe condizioni, equivalenti a un commento precedentemente dichiarato illecito, nonché di valutare se tale ingiunzione produca effetti a livello globale ai sensi del diritto internazionale.

I megadati (*big data*) rappresentano una questione di cruciale rilevanza nei mercati digitali. I servizi *online* commercializzati come gratuiti comportano in realtà un corrispettivo sotto forma di informazioni da parte degli utenti, con la conseguente costituzione di patrimonio di dati nelle mani del fornitore. Un'altra modalità di raccolta è quella della trasmissione mediante apparecchiature connesse alla rete. Varie sono le ragioni della loro rilevanza*:* il mercato interno e l'utilizzazione a fini commerciali da parte delle imprese, il contributo al miglioramento della qualità del settore pubblico, i rischi di discriminazione nella loro utilizzazione[95].

---

[92] Sentenza *Google CNIL*.

[93] Sentenza della Corte (Grande Sezione) del 24 settembre 2019, Causa C-136/17, *GC/CNIL*, ECLI:EU:C:2019:773.

[94] Sentenze della Corte di giustizia del 3 ottobre 2019, causa C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland*, ECLI:EU:C:2019:821. Per un commento, v. E. ROSATI, *Material, personal and geographic scope of online intermediaries' removal obligations beyond Glawischnig-Piesczek (C-18/18) and defamation*, in *European Intellectual Property Review*, 2019, p. 672 ss.; M. MONTI, *La Corte di giustizia, la direttiva e-commerce e il controllo contenutistico online: le implicazioni della decisione C 18-18 sul discorso pubblico online e sul ruolo di Facebook*, in *Medialaws*, 2019, 15 ottobre 2019; F. CALOPRISCO, *La Corte di giustizia si esprime sulla portata territoriale dell'obbligo di deindicizzare i dati personali online,* in *Annali Aisdue*, Vol. I, Bari, 2020, p. 357 ss.

[95] V. regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR). Tra i tanti, v. G. CAGGIANO, *L'interpretazione del "contesto delle attività di stabilimento" dei responsabili del trattamento dei dati personali* in *Il Diritto dell'informazione e dell'informatica*, 2014, p. 605 ss.; F. BESTAGNO, *Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali* in *Il Diritto dell'Unione Europea*, 2015, p. 25 ss.; V. SALVATORE, *La Corte di giustizia restituisce (temporaneamente) agli Stati membri la competenza a valutare l'adeguatezza del livello di protezione dei dati personali soggetti a trasferimento verso gli Stati Uniti*, in *Studi sull'integrazione europea*, 2015, p. 623 ss.; F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona*, in *Rivista di diritto internazionale*, 2016, p. 690 ss.; G. M. RUOTOLO, *I dati non personali: l'emersione dei big data nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 2018, p. 97 ss.

Gli strumenti normativi sui dati adottati si limitano in massima parte a disciplinare il trattamento dei dati "personali", senza tener conto di una serie di peculiarità dei *big data*, tra cui la loro frequente non riconducibilità ad individui determinati.

I dati non personali sono identificati *a contrario* rispetto ai dati personali, definiti dal GDPR[96]. Alla luce del quadro normativo esistente è dubbia l'applicabilità della disciplina generale sulla tutela dei dati alle informazioni che siano raccolte *ab origine* in forma anonima o rese tali a seguito di un procedimento di cancellazione di ogni riferimento alla persona alla quale si riferiscono[97]. Sulla circolazione dei dati non personali, il regolamento 2018/1807/UE intende superare i limiti posti dalle legislazioni nazionali che comportano obblighi di localizzazione dei dati in una determinata area geografica e eliminare gli ostacoli tecnici, giuridici e contrattuali alla mobilità dei dati intra-UE. Tali limiti provocano scarsa concorrenza nell'ambito dei servizi di trattamento di dati e costituiscono un freno all'innovazione, in contrasto con i generali principi europei di libertà di prestazione dei servizi e diritto di stabilimento: "libera circolazione dei dati diversi dai dati personali all'interno dell'Unione stabilendo disposizioni relative agli obblighi di localizzazione dei dati, alla messa a disposizione dei dati alle autorità competenti e alla portabilità dei dati per gli utenti professionali" (art. 1)

Il regolamento si applica alle attività di trattamento di dati elettronici non personali se (a) fornite come servizio ad utenti residenti o stabiliti nell'Unione, o (b) effettuate da una persona fisica o giuridica residente o stabilita nell'Unione per le proprie esigenze (art. 2). Gli obblighi di localizzazione dei dati, in particolare, sono "vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità" (art. 4). Resta però salva la facoltà delle autorità nazionali di ottenere l'accesso ai dati per l'esercizio delle proprie funzioni. La Commissione europea, infine, promuove lo sviluppo di codici di condotta "al fine di contribuire a un'economia dei dati competitiva basata sui principi della trasparenza e dell'interoperabilità".

Come abbiamo detto, i *big data* possono provenire dall'amministrazione pubblica ed essere utili per i cittadini e le imprese. All'apertura dei dati e al riutilizzo

[96] Definiti come "qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato')" e ritiene a tal fine "identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale" (art. 4 GDPR).

[97] Diverso è il concetto di pseudonimizzazione che rientra nel campo di applicazione del GDPR: "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile" (*ivi*, art. 4). La pseudonimizzazione e la cifratura dei dati personali rientrano tra le misure di sicurezza (*ivi*, art. 32). In tal caso, è lecito il trattamento per finalità diverse dal consenso raccolto (*ivi*, art. 6).

dell'informazione del settore pubblico è dedicata la direttiva 2019/1024 (PSI)[98] che tiene conto dei cambiamenti tecnologici e sociali e della normativa di riferimento sulla gestione dei dati nel GPDR. La valorizzazione del patrimonio informativo è una della priorità della strategia, arrivando a definire un quadro normativo volto a incoraggiare ed agevolare il riutilizzo dei dati prodotti dal settore pubblico, imponendo vincoli minimi dal punto di vista giuridico, tecnico e finanziario. L'obbligo di concedere il riutilizzo viene esteso ai dati in possesso delle **imprese,** prodotti nello svolgimento di servizi di interesse economico generale (SIEG) nei settori dell'acqua, energia, trasporti e servizi postali (art. 1, par. 1). La direttiva estende il riutilizzo ai **"dati dinamici"** vale a dire i "documenti in formato digitale, soggetti ad aggiornamenti frequenti o in tempo reale, in particolare a causa della loro volatilità o rapida obsolescenza" (art. 2)[99]. Viene inoltre assicurata la riutilizzabilità di particolari **"dati pubblici di elevato valore"** in quanto idonei alla creazione di servizi ed applicazioni a valore aggiunto e di posti di lavoro "dignitosi e di alta qualità" (art. 2). Anche ai sensi della nuova direttiva, la disciplina del riutilizzo non potrà comportare la diffusione né di dati personali ai sensi delle pertinenti disposizioni UE e nazionali, né di dati sensibili in quanto coperti da segretezza nell'interesse nazionale o da riservatezza per ragioni commerciali (art. 1, par. 2 e par. 4).

Al fine di evitare che il riutilizzo possa portare a fenomeni distorsivi della concorrenza, viene introdotto il **divieto di diritti esclusivi,** prevedendosi che "[i] documenti possono essere riutilizzati da tutti gli operatori potenziali sul mercato, anche qualora uno o più operatori stiano già procedendo allo sfruttamento di prodotti a valore aggiunto basati su tali documenti. I contratti o gli altri accordi tra gli enti pubblici o le imprese pubbliche in possesso dei documenti e terzi non stabiliscono diritti esclusivi. Tuttavia, se per l'erogazione di un servizio d'interesse pubblico è necessario un diritto esclusivo, la fondatezza del motivo per l'attribuzione di tale diritto esclusivo è soggetta a riesame periodico, comunque con scadenza triennale" (art. 12).

Il riutilizzo è di base **gratuito** (art. 6, mentre potrà essere autorizzato il recupero dei **costi marginali** sostenuti per la riproduzione, messa a disposizione e divulgazione dei documenti, nonché per l'anonimizzazione di dati personali o per le misure adottate per proteggere le informazioni commerciali a carattere riservato. Le deroghe a tale principio vengono limitate agli enti pubblici che devono generare proventi per coprire una parte sostanziale dei costi inerenti lo svolgimento dei propri compiti di servizio pubblico, le biblioteche, i musei e gli archivi, nonché le imprese pubbliche (salvo eccezioni indicate all'art. 14). Per enti ed imprese pubbliche, spetterà a ciascuno Stato membro il compito di definire l'importo delle tariffe applicabili secondo criteri oggettivi, trasparenti e verificabili.

[98] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (rifusione).

[99] Si tratta ad esempio dei dati ambientali, relativi ai traffici satellitari, meteorologici ed ai dati generati da sensori, il cui valore economico dipende dall'immediata disponibilità dell'informazione e da regolari aggiornamenti. Per tale categoria di dati, il riutilizzo dovrà avvenire mediante accesso in tempo reale ed interfacce per programmi applicativi (API).

Il riutilizzo non potrà essere soggetto a condizioni, a meno che esse non siano obiettive, proporzionate, non discriminatorie e giustificate sulla base di un obiettivo di interesse pubblico. Si prevede inoltre che gli Stati membri incentivino l'utilizzo di **licenze *standard*** (art. 8). I dati dovranno essere resi disponibili, leggibili meccanicamente ed accessibili mediante API; eventuali condizioni di riutilizzo dovranno essere compatibili con le licenze aperte *standard*[100]. Diverranno oggetto di riutilizzo anche i **dati prodotti nell'ambito della ricerca finanziata con fondi pubblici**. Si tratta dei "documenti in formato digitale, diversi dalle pubblicazioni scientifiche, raccolti o prodotti nel corso della ricerca scientifica e utilizzati come elementi di prova nel processo di ricerca, o comunemente accettati nella comunità di ricerca come necessari per convalidare le conclusioni e i risultati della ricerca" (art. 2). I dati saranno riutilizzabili a fini commerciali o non commerciali "nella misura in cui tali ricerche sono finanziate con fondi pubblici e ricercatori, organizzazioni che svolgono attività di ricerca e organizzazioni che finanziano la ricerca li hanno già resi pubblici attraverso una banca dati gestita a livello istituzionale o su base tematica" (art. 10).

13. Il "pacchetto contratti digitali" comprende due direttive: la direttiva 2019/770, sui contratti di fornitura di contenuti digitali e di servizi digitali, e la direttiva 2019/771 sui contratti di vendita di beni[101]. Entrambe finalizzate ad armonizzare i requisiti per la vendita, nonché gli strumenti di ricorso attivabili in caso di mancata conformità.

La direttiva 2019/770 sul contenuto digitale si pone principalmente l'obiettivo di stabilire norme comuni sui contratti che riguardano contenuto digitale (e quindi i dati prodotti e forniti in formato digitale) o servizi digitali. Le nuove regole si applicano sia nel caso in cui la fornitura del contenuto digitale è effettuata a fronte del pagamento di un prezzo, sia qualora essa venga effettuata a fronte della fornitura dei dati personali del consumatore.

La direttiva 2019/771 contiene innovazioni in tema di contratti di vendita a distanza con i consumatori; riguarda anche le ipotesi di somministrazione di acqua, gas ed elettricità e che ricadono sotto la sua applicazione anche i "beni con elementi digitali" ossia quei beni che incorporano o sono interconnessi con contenuti digitali o servizi digitali (Internet delle Cose o *smart device*), la cui mancanza impedirebbe lo svolgimento delle funzioni del bene.

[100] L'elenco di tale tipologia di dati, che verrà definito dalla Commissione europea nei prossimi due anni a seguito di apposite consultazioni, potrebbe includere in particolare "i codici di avviamento postale, le mappe e le carte nazionali e locali (dati geo-spaziali), il consumo energetico e le immagini satellitari (dati relativi all'osservazione della terra e all'ambiente), i dati in situ provenienti da strumenti e previsioni meteorologiche (dati meteorologici), gli indicatori demografici e economici (dati statistici), i registri delle imprese e gli identificativi di registrazione (dati relativi alle imprese e alla proprietà delle imprese), la segnaletica stradale e le vie navigabili interne (dati relativi alla mobilità)" (considerando 66).

[101] Le nuove regole in materia di vendite di beni si applicheranno sia alle vendite *online*, sia alle vendite tradizionali frontali. Il pacchetto si propone di ammodernare il quadro normativo risalente al 1999.

Per quanto riguarda le responsabilità del fornitore, i diritti degli utenti e le garanzie/rimedi, i due atti seguono una falsariga, con alcune variazioni.

Nella direttiva 2019/770, al fornitore spetta la responsabilità, con l'inversione dell'onere della prova, per i difetti di conformità del prodotto: conformità alla descrizione e all'uso dichiarato dal fornitore; consegna degli accessori richiesti e dei relativi aggiornamenti, specie gli aggiornamenti di sicurezza (salvo che il consumatore non provveda alla loro installazione entro un termine ragionevole). Al consumatore sono riconosciuti, in caso di difformità dai requisiti, il diritto al recesso immediato dal contratto, il diritto al ripristino della conformità o alla riduzione del prezzo ed il diritto alla risoluzione del contratto, con conseguente rimborso delle somme pagate; il diritto alla portabilità dei dati forniti o creati dal consumatore durante l'utilizzo del contenuto digitale o del servizio, i quali dovranno essere messi a disposizione in un formato di uso comune e leggibile da dispositivo automatico.

Nella direttiva 2019/771, è stabilito che i medesimi beni debbano essere conformi ai requisiti soggettivi dichiarati dal fornitore nonché agli ulteriori requisiti (art. 7). Se i beni comprendono elementi digitali, vi sono degli obblighi del fornitore di fornire gli aggiornamenti, compresi quelli di sicurezza, necessari a far mantenere al bene i requisiti di conformità, ferma restando l'esenzione di responsabilità del fornitore qualora il consumatore non installi gli aggiornamenti entro un ragionevole periodo di tempo. Anche in tale testo sono previsti diversi rimedi per il consumatore: la possibilità di richiedere il ripristino della conformità del bene (a scelta tra riparazione o sostituzione dello stesso) o la riduzione del prezzo, la possibilità di rifiutarsi di pagare il prezzo fin quando il venditore non abbia adempiuto alle sue obbligazioni, l'eventuale risoluzione del contratto di vendita, con conseguente rimborso del prezzo.

14. La direttiva (UE) 2019/2161[102], che rientra nel quadro normativo del "New Deal" per i consumatori, estende ai contenuti digitali e ai servizi digitali le direttive relative alle pratiche commerciali sleali (2005/29/CE) e ai diritti dei consumatori (2011/83/UE)[103].

Per le esigenze della tutela del consumatore, oltre alla base giuridica dell'art. 114 TFUE, il riferimento specifico è all'art. 169 TFUE secondo cui l'Unione contribuisce "a promuovere e a tutelare la salute, la sicurezza e gli interessi economici dei consumatori". Il suo primo paragrafo si riferisce a misure rivolte ad integrare, promuovere e supportare le politiche ed il sistema di misure statali predisposte dagli Stati membri. Il suo secondo paragrafo individua gli strumenti con cui l'Unione può perseguire tali obiettivi; in

[102] Direttiva (UE) 2019/2161 del Parlamento europeo e del Consiglio del 27 novembre 2019 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori.

[103] Tali modifiche devono essere lette anche in relazione con la direttiva (UE) 2019/770 e la direttiva (UE) 2019/771 poiché l'insieme normativo comporta l'eliminazione di qualsiasi irragionevole differenza nella regolamentazione dei beni tradizionali e dei servizi/contenuti digitali.

particolare la lett. a) non conferisce un potere autonomo ma si riferisce di nuovo all'art. 114 TFUE.

Nella Comunicazione New Deal[104], la Commissione afferma che resta impregiudicata la competenza statale a tracciare i confini delle professioni, ma si prevede espressamente l'obbligo della piattaforma di specificare se il terzo che offre beni, servizi o contenuto digitale è un professionista, sulla base della dichiarazione del terzo stesso; se al contratto concluso si applicano o meno i diritti dei consumatori derivanti dalla legislazione dell'Unione; a quale professionista spetti la responsabilità. Ciò corrisponde all'obbligo delle piattaforme di comunicare ai consumatori se il professionista responsabile è il venditore e/o la piattaforma online (art. 6 *bis*); se del caso, il modo in cui gli obblighi relativi al contratto sono ripartiti tra il terzo che offre i beni o i servizi e il fornitore del mercato *online*.

Sulla qualificazione del fornitore del servizio, la disposizione della direttiva (art. 4) solleva perplessità, in quanto non è soggetta a verifica neanche della stessa piattaforma e, soprattutto, manca una sicura definizione legislativa del concetto di attività professionale. Nella sentenza *Kamenova*[105], la Corte di giustizia ha chiarito che spetta al giudice nazionale stabilire, caso per caso, sulla base di tutti gli elementi di fatto di cui dispone, se una persona fisica abbia agito nel quadro della sua attività commerciale, industriale, artigianale o professionale, verificando, in particolare, se la vendita sia stata effettuata in modo organizzato, se abbia carattere di regolarità o fini di lucro, se l'offerta sia concentrata su un numero limitato di prodotti, nonché esaminare lo *status* giuridico e le competenze tecniche del venditore. Tuttavia, l'ibridazione prodotta dalla economia collaborativa tra le figure di professionista e consumatore (*prosumer*) non consente di chiarire l'entità degli obblighi giuridici a carico del "privato" che decida di offrire un bene o servizio in via non "professionale" ma comunque neanche occasionale[106].

---

[104] COM(2018) 183 final, 11 aprile 2018, Un "New Deal" per i consumatori.

[105] Sentenza della Corte (Quinta Sezione) del 4 ottobre 2018, *Evelina Kamenova*, causa C-105/17, ECLI:EU:C:2018:808. Una persona fisica che pubblica su un sito Internet, contemporaneamente, un certo numero di annunci per la vendita di beni nuovi e d'occasione, quale la convenuta nel procedimento principale, può essere qualificata come "professionista", e una siffatta attività può costituire una "pratica commerciale", soltanto qualora tale persona agisca nel quadro della sua attività commerciale, industriale, artigianale o professionale, cosa che spetta al giudice del rinvio verificare, alla luce di tutte le circostanze rilevanti del caso di specie.

[106] Nella sentenza del 25 gennaio 2018, causa C-498/16, *Schrems II,* ECLI:EU:C:2018:37, la Corte ha anche affermato che le competenze assunte dall'interessato in un determinato settore (nella specie: la protezione dei dati personali) non fossero idonee a fargli perdere la qualifica di consumatore, giacché tale nozione rileva solo in senso oggettivo e non soggettivo. Un utilizzatore di un account Facebook privato non perde la qualità di "consumatore", allorché pubblica libri, tiene conferenze, gestisce siti Internet, raccoglie donazioni e si fa cedere i diritti da numerosi consumatori al fine di far valere in giudizio tali diritti; l'azione di un consumatore può essere diretta a far valere, dinanzi al giudice del luogo in cui questi è domiciliato, non soltanto diritti propri ma anche diritti ceduti da altri consumatori domiciliati nello stesso Stato membro, in altri Stati membri oppure in Stati terzi (regolamento (CE) n. 44/2001 del Consiglio, del 22 dicembre 2000, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, articoli 15 e 16, par. 1).

Alle pratiche commerciali sleali, la direttiva 2019/2161 aggiunge quattro fattispecie tipicamente collegate al contesto digitale: la *prima fattispecie* nella quale un professionista fornisce risultati di ricerca in risposta a una ricerca *online* del consumatore senza che sia chiaramente indicato ogni eventuale annuncio pubblicitario a pagamento o eventuali pagamenti specifici effettuati per ottenere una classificazione migliore dei prodotti all'interno di tali risultati; la *seconda* nella quale un professionista rivende ai consumatori biglietti per eventi che lo stesso ha acquistato utilizzando strumenti automatizzati per eludere qualsiasi limite imposto riguardo al numero massimo di biglietti che una persona può acquistare, o qualsiasi altra norma relativa all'acquisto di biglietti; la *terza* nella quale un professionista afferma che le recensioni di un prodotto sono inviate da consumatori che hanno effettivamente utilizzato o acquistato il prodotto senza adottare misure ragionevoli e proporzionate per verificare che le recensioni provengano realmente da tali consumatori; la *quarta* fattispecie in cui un professionista invia recensioni di consumatori false o fornisce informazioni false in merito a recensioni di consumatori o ad apprezzamenti sui *social media* al fine di promuovere prodotti.

Sulle riduzioni di prezzo, la direttiva 2019/2161 detta regole dettagliate: ogni annuncio relativo alla riduzione di prezzo dovrà specificare il prezzo precedentemente applicato dallo stesso professionista per un determinato periodo di tempo antecedente a tale riduzione. Il criterio di rilevanza del prodotto rispetto alla ricerca effettuata dall'utente deve essere indicato dalle piattaforme, in particolare quali criteri determinano la successione (*ranking*) dei prodotti suggeriti e mostrati in evidenza o suggeriti. Le piattaforme saranno tenute ad indicare le modalità con cui sono stati catalogati i prodotti come più votati, più desiderati, più acquistati, più regalati etc. Per quanto concerne l'utilizzo di recensioni *online*, i professionisti devono informare i consumatori se hanno adottato procedure di verifica idonee a garantire che provengano da consumatori che hanno effettivamente acquistato o utilizzato i prodotti in questione e quali sono le modalità di tali verifiche. In ogni caso, dovranno imporre di indicare i risultati di ricerca che contengono "posizionamenti o inclusioni a pagamento".

La categoria dei servizi digitali "gratuiti", prevedendo che le normative in materia di contratti a distanza trovino applicazione anche quando il professionista fornisce un contenuto digitale mediante un servizio digitale al consumatore che ricambia dati personali al professionista, tranne i casi in cui tali dati personali siano trattati dal professionista esclusivamente ai fini della fornitura del contenuto digitale in questione.

Infine, la direttiva prevede una maggiore armonizzazione e semplificazione dei criteri utilizzati per stabilire il livello delle sanzioni in caso di violazioni; i diritti nei confronti di pratiche commerciali sleali (es: *marketing* aggressivo); l'obbligo di informazioni chiare in caso di riduzione dei prezzi; l'introduzione di una definizione della differenza di qualità dei prodotti (*dual quality*) tra i casi di pratica ingannevole[107].

[107] In particolare, è stata inserita nell'art. 6, comma 2 lettera c) della direttiva 2005/29/CE la seguente definizione di "*dual quality*": una qualsivoglia attività di *marketing* che promuova un bene, in uno Stato membro, come identico a un bene commercializzato in altri Stati membri,

Strategia del Mercato Unico digitale
(completato con i provvedimenti adottati)
Allegato a COM (2018) 320 final

Uso della banda di frequenza 470-790 MHz
Decisione (UE) 2017/899 del Parlamento europeo e del Consiglio, del 17 maggio 2017, relativa all'uso della banda di frequenza 470-790 MHz nell'Unione

Portabilità transfrontaliera di servizi di contenuti online
Regolamento (UE) 2017/1128 del Parlamento europeo e del Consiglio, del 14 giugno 2017, relativo alla portabilità transfrontaliera di servizi di contenuti online nel mercato interno

Mercati del roaming all'ingrosso
Regolamento (UE) 2017/920 del Parlamento europeo e del Consiglio, del 17 maggio 2017che modifica il regolamento (UE) n. 531/2012 per quanto riguarda le norme sui mercati del roaming all'ingrosso

Usi consentiti di opere protette dal diritto d'autore per le persone con difficoltà nella lettura di testi (trattato di Marrakech)
Direttiva (UE) 2017/1564 del Parlamento europeo e del Consiglio, del 13 settembre 2017, relativa a taluni utilizzi consentiti di determinate opere e di altro materiale protetto da diritto d'autore e da diritti connessi a beneficio delle persone non vedenti, con disabilità visive o con altre difficoltà nella lettura di testi a stampa, e che modifica la direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione

Regolamento (UE) 2017/1563 relativo allo scambio transfrontaliero tra i paesi dell'UE e i paesi terzi di copie in formato accessibile di determinate opere e di altro materiale protetto da diritto d'autore e da diritti connessi, a beneficio delle persone non vedenti, con disabilità visive o con altre difficoltà nella lettura di testi a stampa

Promozione della connettività Internet nelle comunità locali
Regolamento (UE) 2017/1953 del Parlamento europeo e del Consiglio, del 25 ottobre 2017, che modifica i regolamenti (UE) 1316/2013 e (UE) n. 283/2014 per quanto riguarda la promozione della connettività internet nelle comunità locali

Cooperazione per la tutela dei consumatori
Regolamento (UE) 2017/2394 del Parlamento europeo e del Consiglio, del 12 dicembre 2017, sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori e che abroga il regolamento (CE) n. 2006/2004

Blocchi geografici ingiustificati
Regolamento (UE) 2018/302 del Parlamento europeo e del Consiglio, del 28 febbraio 2018, recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno e che modifica i regolamenti (CE) n. 2006/2004 e (UE) 2017/2394 e la direttiva 2009/22/CE (Testo rilevante ai fini del SEE)

Imposta sul valore aggiunto per il commercio elettronico

---

mentre questo bene ha una composizione o caratteristiche significativamente diverse, salvo laddove ciò sia giustificato da fattori legittimi e oggettivi.

Direttiva (UE) 2017/2455 del Consiglio, del 5 dicembre 2017, che modifica la direttiva 2006/112/CE e la direttiva 2009/132/CE per quanto riguarda taluni obblighi in materia di imposta sul valore aggiunto per le prestazioni di servizi e le vendite a distanza di beni
Regolamento (UE) 2017/2454 del Consiglio, del 5 dicembre 2017, che modifica il regolamento (UE) n. 904/2010 relativo alla cooperazione amministrativa e alla lotta contro la frode in materia d'imposta sul valore aggiunto

Consegna transfrontaliera dei pacchi
Regolamento (UE) 2018/644 del Parlamento europeo e del Consiglio, del 18 aprile 2018, relativo ai servizi di consegna transfrontaliera dei pacchi

Servizi di media audiovisivi
Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio del 14 novembre 2018 recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi

Contratti di fornitura di contenuto digitale
Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali

Contratti di vendita a distanza di beni
Direttiva (UE) 2019/771 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di vendita di beni, che modifica il regolamento (UE) 2017/2394 e la direttiva 2009/22/CE, e che abroga la direttiva 1999/44/CE

Codice europeo delle comunicazioni elettroniche
Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche (rifusione)

Organismo dei regolatori europei delle comunicazioni elettroniche
Regolamento (UE) 2018/1971 che istituisce l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC) e l'Agenzia di sostegno al BEREC

Diritto d'autore nel mercato unico digitale
Direttiva 2019/790, del Parlamento europeo e del Consiglio del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale

Organismi di radiodiffusione
Direttiva (UE) 2019/789 del Parlamento europeo e del Consiglio del 17 aprile 2019 che stabilisce norme relative all'esercizio del diritto d'autore e dei diritti connessi applicabili a talune trasmissioni online degli organismi di diffusione radiotelevisiva e ritrasmissioni di programmi televisivi e radiofonici e che modifica la direttiva 93/83/CEE del Consiglio

Imposta sul valore aggiunto applicata alle pubblicazioni elettroniche
Direttiva (UE) 2018/1713 DEL CONSIGLIO del 6 novembre 2018 che modifica la direttiva 2006/112/CE per quanto riguarda le aliquote dell'imposta sul valore aggiunto applicate a libri, giornali e periodici

Protezione dei dati personali da parte delle istituzioni e degli organismi dell'Unione
Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e

degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE

Sportello digitale unico
Regolamento (UE) 2018/1724 del Parlamento europeo e del Consiglio, del 2 ottobre 2018, che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE) n. 1024/2012

Regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali
Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea

Cibersicurezza
Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013

Lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti
Direttiva 2019/713, del Parlamento Europeo e del Consiglio del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, che sostituisce la decisione quadro 2001/413/GAI del Consiglio

Impresa comune europea di calcolo ad alte prestazioni
Regolamento (UE) n. 2018/1488 che istituisce l'impresa comune per il calcolo ad alte prestazioni europeo

Equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online
Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online

Riutilizzo delle informazioni del settore pubblico
Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (rifusione)

Messa in opera e al funzionamento del nome di dominio di primo livello .eu
Regolamento (UE) 2019/517 del Parlamento europeo e del Consiglio, del 19 marzo 2019, relativo alla messa in opera e al funzionamento del nome di dominio di primo livello .eu, che modifica e abroga il regolamento (CE) n. 733/2002 e abroga il regolamento (CE) n. 874/2004 della Commissione

Vita privata e comunicazioni elettroniche (e-privacy)
Proposta di Regolamento del Parlamento europeo e del Consiglio, relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche). COM/2017/010 final, 10.1.2017

Brevi osservazioni sulle recenti tendenze evolutive della giurisprudenza della Corte di Giustizia dell'Unione europea sulla protezione dei dati personali[*]

DI LUCIA SERENA ROSSI[**]

1. Il tema della protezione dei dati personali e, più in generale, la tutela dei diritti fondamentali in confronto a tutti i nuovi mezzi di comunicazione sono oggetto di sempre più frequente di attenzione da parte della Corte di giustizia dell'Unione europea. Dato lo spazio limitato che giustamente è riservato ad un intervento ad un Convegno, queste brevi note introduttive si limiteranno ad illustrare alcune tendenze che emergono dalla più recente giurisprudenza della Corte, con l'avvertenza che ancora molte e importanti pronunce saranno rese nei prossimi mesi nella materia in oggetto.

Se è normale che con il crescere della legislazione aumentino anche i problemi di interpretazione, con l'adozione del GDPR, le questioni si sono moltiplicate. Naturalmente, oltre alle questioni di interpretazione delle norme europee e quesiti sulla compatibilità delle leggi degli Stati membri nell' attuazione di dette norme, possono porsi, come già accaduto nel caso *Digital Rights Ireland*[1], anche problemi di validità della legislazione dell'Unione, alla luce della protezione dei diritti fondamentali ed in particolare della Carta dei diritti fondamentali.

La Corte si trova pertanto ad affrontare un gran numero di questioni giuridiche che riguardano le attività di acquisizione, conservazione e commercio di dati o metadati. Queste attività, che possono contribuire a profilare un individuo, entrando, anche a sua insaputa, nella sua vita privata, sono svolte da operatori pubblici o privati, talvolta anche in conseguenza di un obbligo di conservazione imposto da certi Stati membri ai gestori delle linee telefoniche. Ma ancora più frequentemente i problemi sorgono con riferimento all'utilizzo dei dati da parte dei gestori delle piattaforme, anche perché queste ultime spesso sono filiali stabilite in Europa di società americane, cui le autorità del loro Paese chiedono il trasferimento dei dati.

Nella disciplina di questa materia a livello dell'Unione e nella giurisprudenza della CGUE, si registra un'evoluzione, cu cui ha avuto un impatto molto significativo la Carta dei diritti fondamentali. Infatti, le prime direttive sui dati personali vertevano principalmente sulla libera circolazione di questi ultimi e miravano ad armonizzare i

[*] Questo testo costituisce la trascrizione rivista di un intervento pronunciato al Convegno "Mercato unico digitale, dati personali e diritti fondamentali", tenutosi il 16 dicembre 2019 presso l'Università degli Studi di Milano.

[**] Giudice alla Corte di Giustizia dell'Unione europea. Le opinioni espresse sono strettamente personali e non coinvolgono la Corte

[1] Sentenza dell'8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland e a*., EU:C:2014:238.

sistemi di protezione nazionali, per evitare che divergenze profonde fra gli stessi potessero giustificare gli Stati membri ad ostacolare il commercio di tali dati. Con il passare del tempo, sia perché emergevano in maniera crescente i rischi per la sfera soggettiva degli individui, sia perché, assieme al Trattato di Lisbona, è entrata in vigore anche la Carta dei diritti fondamentali, il *focus* della giurisprudenza si è spostato dal mercato alla tutela dei diritti.

Ma anche con riferimento a tale ambito, si osserva un'ulteriore evoluzione. Infatti, dopo l'affermazione, anche a livello giurisprudenziale del valore della Carta, il problema con cui la Corte deve confrontarsi è il bilanciamento, non più solo fra mercato e diritti, ma anche fra vari diritti confliggenti. In quest'ultimo caso, si tratta di un bilanciamento complesso, che definirei "*multifocale*", perché, molto spesso, non sono in gioco solo due diritti contrapposti, ma una pluralità di diversi diritti, nonché di soggetti interessati. Ad esempio, quando, da un lato si pongono il diritto all'oblio o il diritto alla privacy, d'altro lato, possono contrapporsi la libertà di espressione e di opinione, la libertà di stampa, ma anche un terzo diritto, quello del pubblico, in generale, a ricevere informazioni.

Questo bilanciamento, quindi, è -e sarà sempre più- l'essenza della giurisprudenza nella materia in esame, non solo della Corte di Lussemburgo, ma anche di quella di Strasburgo (com'è noto, ai sensi dell'art 52.3 della Carta, la seconda costituisce standard minimo per la prima) e delle Corti costituzionali degli Stati membri. Quindi, anche se -e proprio perché- i diritti sono in principio "tutti tutelati da tutti", il problema, che va risolto caso per caso, è il diverso mix, ovvero come bilanciare i vari diritti.

Sorge allora il problema di individuare "chi fa cosa" fra questa pluralità di giurisdizioni, poiché non è detto che il bilanciamento fra tanti diritti in gioco venga effettuato allo stesso modo, con il rischio che, a seconda di chi giudica, venga data una risposta diversa. Questa situazione richiede un dialogo e uno scambio di informazioni fra le Corti.

Un esempio recente, che illustra la complessità della situazione, è costituito da due recenti ordinanze con cui la Corte costituzionale tedesca si è pronunciata tema del diritto all'oblio [2]. La prima causa riguardava la pubblicazione online, da parte dello *Spiegel*, dei propri archivi, dai quali era risultata una notizia di reato risalente al 1981; nel secondo caso, invece, si trattava di un'intervista televisiva ad un datore di lavoro, il quale aveva esercitato pratiche scorrette nei confronti dei propri dipendenti, intervista che era stata poi trascritta e diffusa online.

La Corte tedesca ha deciso in modo differente le due questioni. Nel primo caso, considerando che non sussiste una normativa condivisa in materia di *media privilege*, la Corte ha riconosciuto una certa discrezionalità in capo agli Stati membri e ha ritenuto applicabile la costituzione nazionale. Nel secondo caso, invece, considerando che in materia di trattamento dei dati personali è stata effettuata un'armonizzazione legislativa a livello dell'Unione, la Corte ha ritenuto necessario lasciare spazio al primato del diritto

[2] Su cui v. Rossi, L.S. *«Il "nuovo corso" del Bundesverfassungsgericht nei ricorsi diretti di costituzionalità: bilanciamento fra diritti confliggenti e applicazione del diritto dell'Unione»*, in Federalismi, n. 3/2020, p. iv ss.

di quest'ultima, concludendo che il parametro di valutazione non è la costituzione nazionale, ma la Carta. Tuttavia, la Corte costituzionale ha deciso di applicare direttamente la Carta, non avendo dubbi circa la sua interpretazione e non ritenendo, dunque, necessario interpellare la Corte di giustizia.

Ora, se nel caso specifico non si può rimproverare al Bundesverfassungsgericht alcun errore nell'applicazione della Carta, è evidente che non si può escludere, in via generale, che l'avocazione della decisione sulla compatibilità con il diritto comunitario da parte delle Corti costituzionali o supreme degli Stati membri possa comportare rischi di applicazioni difformi degli stessi principi e diritti.

Se è dunque necessario un coordinamento spontaneo fra giurisdizioni, a mio avviso un tale coordinamento dovrebbe tenere conto di un fattore importante: quando si tratta di una norma armonizzata, anche il bilanciamento dovrebbe seguire, in linea di massima, criteri comuni, pur tenendo conto delle diverse situazioni. Inoltre, se l'interpretazione uniforme delle norme dell'Unione europea, inclusa la Carta, spetta esclusivamente alla Corte di Giustizia, l'applicazione di quelle norme è compito di tutti i giudici nazionali, i quali a loro volta devono tenere conto, in tale applicazione, dei criteri enunciati dalle rispettive Corti costituzionali.

2. Ciò premesso, ricordo qui, solo brevemente, alcune fra le più importanti sentenze recenti della Corte di giustizia, che contribuiscono a creare un quadro in costante evoluzione e precisazione della materia in esame.

In primo luogo, la Corte si trova spesso ad interpretare le nozioni fissate dalla legislazione dell'Unione, in un processo di qualificazione che deve a volte colmando lacune di tale legislazione.

Nella sentenza *Google Spain*[3], la Corte di giustizia ha concluso che la indicizzazione è un trattamento di dati personali perché consente la profilazione dell'individuo. Google si difendeva dicendo di non essere responsabile dei contenuti pubblicati in rete, in quanto si occupava solo della loro indicizzazione e non della loro messa in rete. La Corte, però, ha ritenuto che da un lato, è compito del gestore sopprimere i dati e, dall'altro, che anche la conservazione lecita dei dati, può, con il passare del tempo, diventare incompatibile con il diritto alla privacy. In questa sentenza molto coraggiosa la Corte ha anche affermato che, anche in assenza di un danno, sussiste il diritto alla cancellazione dei dati, ammettendo però alcune eccezioni legate al ruolo ricoperto dalla persona (in particolare, un ruolo pubblico) o alla presenza di un preponderante interesse del pubblico.

Nella stessa sentenza la Corte ha precisato anche che, nonostante Google abbia una sede in un altro Stato (la sua sede principale è al di fuori dell'Unione europea), a dirimere la controversia sono competenti il giudice e le autorità dello Stato in cui ha sede la società che vende la pubblicità, la quale consente di alimentare il motore di ricerca. Il passo successivo è stato compiuto dalla sentenza *Schrems*[4], in cui la Corte ha affermato che il trasferimento verso gli Stati Uniti, nonostante il c.d. *Safe Harbor*, non pregiudica il potere

[3] Sentenza del 13 maggio 2014, C-131/12, *Google Spain e Google*, EU:C:2014:317.
[4] Sentenza del 6 ottobre 2015, C-362/14, *Schrems*, EU:C:2015:650.

dell'autorità di uno Stato dell'Unione di garantire l'accesso ai dati su richiesta dell'interessato. Non mi soffermo su questa sentenza, notissima e molto commentata, ma osservo che essa costituisce un tassello fondamentale nel percorso che sta seguendo la Corte anche in sentenze ora pendenti. Diventa sempre più evidente che l'Unione europea, a differenza degli USA, ha un approccio alle libertà del trattamento dei dati basato sui diritti e sui controlli, un approccio, comune anche alle Corti nazionali.

Nella sentenza *Fashion ID*[5] la Corte si è occupata della questione dei *plug-in*: la Corte li ha qualificati come attività che realizza un trattamento di dati (dal momento che, attraverso di essi, vengono trasferiti *cookies* a Facebook) e, dunque, ha ritenuto il sito coinvolto nella controversia – Fashion ID, appunto – co-responsabile del trattamento, giudicandolo tenuto a rispettare la direttiva 95/46 e, quindi, a fornire tutte le informazioni relative al trattamento dei dati.

In secondo luogo, la Corte si trova ad affrontare un problema estremamente delicato, concernente i poteri degli Stati membri di imporre ad operatori privati la conservazione dei dati personali degli utenti, e poi chiedere l'accesso agli stessi per finalità di pubblica sicurezza. Non è facile trovare un equilibrio fra le esigenze, da un lato, di poter efficacemente lottare contro la criminalità e, dall'altro, di evitare un Grande Fratello che tutto sa di noi.

Nel 2018 è stata pronunciata la sentenza *Ministerio Fiscal*[6] sui gestori telefonici e sulla proporzionalità delle leggi che li obbligano alla conservazione dei dati. La Corte, in questa occasione, ha deciso che una tale legislazione è ammissibile ma deve essere proporzionata alla gravità dei crimini. Anche alcuni casi attualmente pendenti (causa C-623/17 *Privacy International*, cause riunite C-511/18 e C-512/18 *La Quadrature du Net e a*. e causa C-520/18 *Ordre des barreaux francophones et germanophone e a.*) rigiurano in particolare le norme di alcuni Stati membri che obbligano i gestori a mettere a disposizione della polizia i metadati, determinando una sicura ingerenza a priori (si parla di indagini preventive, perché può esigersi che vengano consegnati dati per sospetti criminali). Se da un lato si sono costituite le Associazioni a tutela della privacy, dall'altro, si schierano Associazioni che tutelano i diritti delle persone coinvolte, quali vittime nelle vicende criminose. Ancora una volta il diritto alla privacy dovrà essere bilanciato, in maniera molto attenta ed equilibrata, con numerosi e diversi diritti in gioco.

Il 14 febbraio 2019, nella sentenza *Buivids*[7], si trattava di un interrogatorio di polizia, che era stato filmato e pubblicato su Youtube. In una simile situazione venivano in gioco numerosi diritti: la libertà d'informazione, la tutela dei dati personali, la tutela della segretezza, richiesta dalla polizia. La Corte di giustizia ha lasciato al giudice nazionale la decisione di bilanciare i diritti in conflitto.

In terzo luogo, la Corte continua a precisare il bilanciamento nelle situazioni in cui sono, classicamente, in gioco, da un lato, libertà di espressione o di informazione e,

[5] Sentenza del 29 luglio 2019, C-40/17, *Fashion ID*, EU:C:2019:629.
[6] Sentenza del 2 ottobre 2018, C-207/16, *Ministerio Fiscal*, , EU:C:2018:788.
[7] Sentenza del 14 febbraio 2019, C-345/17, *Buivids*, EU:C:2019:122.

dall'altro, tutela della vita privata. Il 24 settembre 2019 sono state pubblicate due sentenze fondamentali: la sentenza *GC* [8] e la sentenza *Google*[9].

Nella prima pronuncia, relativa al tema della deindicizzazione, viene espressamente affermato che i diritti fondamentali prevalgono sull'interesse economico dell'imprenditore. Nell'applicazione del test di proporzionalità, ovvero nel bilanciamento tra il diritto alla privacy e la libertà d'informazione, la Corte ha sostenuto che, trattandosi di dati sensibili, se il trattamento è "necessario" al fine di garantire al libertà d'informazione, il diritto alla privacy può cedere di fronte all'esigenza di tutelare questa libertà; tuttavia, trattandosi di dati particolarmente sensibili, il trattamento dei dati, per essere ammissibile al fine di consentire la suddetta libertà, deve essere "strettamente necessario". Tale soluzione, in realtà, può generare alcuni problemi applicativi poiché il bilanciamento dovrà essere effettuato dal gestore, il quale, tuttavia, occupandosi solamente dell'indicizzazione, non è necessariamente a conoscenza del contenuto delle informazioni di cui tratta.

Nella seconda pronuncia, invece, si affronta la questione della portata territoriale della deindicizzazione. In particolare, la causa riguardava la libertà di stampa, con riferimento alla quale, non sussistendo una normativa condivisa a livello comunitario, spetta agli Stati membri fissare esenzioni e deroghe. Secondo la Corte, non si può imporre a priori un controllo generale a priori sul trattamento da parte delle piattaforme, nella fattispecie di Google.

Secondo alcuni, quest'ultima pronuncia sarebbe contraddetta da una sentenza del 3 ottobre 2019, la sentenza *Glawischnig*[10], riguardante una parlamentare austriaca del partito dei Verdi, la quale era stata calunniata su Facebook -ed il fatto che si trattasse di una calunnia era stato accertato da un giudice- e aveva chiesto la rimozione delle calunnie. In questo caso, la Corte di giustizia ha ritenuto che, se è pur vero che la piattaforma Facebook non ha l'onere di controllare il contenuto di ciò che viene caricato, nel momento in cui esiste una sentenza di un giudice nazionale, che accerta un'illegalità, la piattaforma è tenuta non soltanto alla cancellazione delle calunnie, ma, addirittura, alla loro cancellazione a livello mondiale. Tale elemento, a prima vista, sembrerebbe contrastare con quanto affermato dalla sentenza *Google*, in merito alla territorialità della deindicizzazione. Tuttavia, non è così: mentre nella pronuncia Google, si trattava di una semplice richiesta formulata da un individuo a vedersi tutelato il diritto all'oblio, nella sentenza *Glawischnig*, era intervenuta una sentenza di un giudice, che presuppone un'indagine e un seguente accertamento. Non vi è dunque alcuna contraddizione fra le due sentenze: a situazioni diverse corrisponde un bilanciamento diverso dei diritti in gioco. Il dritto all'oblio si contempera con la libertà di espressione e con la libertà di stampa, ma quest'ultima non giustifica qualunque violazione e tantomeno il diritto all'odio.

[8] Sentenza del 24 settembre 2019, C-136/17, *GC e a.* (Deindicizzazione di dati sensibili), EU:C:2019:773.
[9] Sentenza del 24 settembre 2019, C-507/17, *Google* (Portata territoriale della deindicizzazione), EU:C:2019:772.
[10] Sentenza del 3 ottobre 2019, *Glawischnig-Piesczek*, C-18/18, EU:C:2019:821.

Va infine rilevato che questioni relative ai dati personali sorgono in maniera crescente anche con riferimento a questioni che riguardano la vita quotidiana dei rapporti fra privati. Nella sentenza *Nowak*[11] è stato considerato che rientrano nella nozione di dati personali le domande le risposte agli esami (nel caso di specie non si trattava di esami universitari ma di colloqui professionali). Di recente, la Corte è stata addirittura consultata, con un rinvio pregiudiziale, a proposito delle telecamere di sorveglianza installate in un condominio[12] ed ha risposto che, salvo violazioni estreme, il criterio della proporzionalità consente di dichiarare che il diritto dell'Unione non si oppone a normative nazionali che consentano simili pratiche.

3. In conclusione, la sfida che si profila, per il diritto e per tutte le Corti, è quella di tenere il passo con un incremento esponenziale della crescita tecnologica, che porta con sé nuove opportunità ma anche nuove minacce.

Se il web si rivolge a tutti e collega tutti, il suo controllo sembra concentrarsi sempre più nelle mani di poche società mondiali, il cui bilancio e il cui potere rivaleggiano ormai con quelli degli Stati. La stessa sovranità degli Stati sembra impotente, perché queste società hanno ormai un potere contrattuale enorme e spesso riescono ad indirizzare la regolamentazione del settore a loro vantaggio. Diventa dunque importante che le autorità di controllo nazionali dello Stato dell'Unione in cui la piattaforma ha la sua sede legale esercitino i loro poteri in maniera adeguata. Nsentenza *Wirtschaftsakademie c. Facebook*[13] è già stato precisato che, visto che Facebook raccoglie dati con i *cookies* e vende pubblicità in Germania, si applica il diritto tedesco e le autorità competenti tedesche possono controllare il rispetto della privacy, l'accesso agli atti, e così via. La Corte si troverà presto a decidere anche sull'estensione dei poteri di dette autorità, con particolare riferimento alla delimitazione del loro ruolo rispetto ai giudici degli Stati membri[14].

Di fronte a queste forze titaniche, l'azione delle istituzioni dell'Unione europea, assieme a quella dei suoi Stati membri, diventa cruciale per offrire agli individui una protezione adeguata. Al momento in cui questo articolo va in bozza, la Corte di Giustizia, con sentenza del 16 luglio 2020, ha dichiarato invalida la decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy. La sentenza avrà un impatto notevole sulla possibilità che Facebook trasferisca dati personali, anche sensibili, al di fuori dell'Unione europea[15].

[11] Sentenza del 20 dicembre 2017, C-434/16, *Nowak*, EU:C:2017:994.
[12] Sentenza dell'11 dicembre 2019, C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA*, EU:C:2019:1064.
[13] Sentenza del 5 giugno 2018, C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388.
[14] Causa C-645/19 *Facebook Ireland*, attualmente pendente
[15] Causa C-311/18 *Data Protection Commissioner c. Facebook Ireland*.

La tutela dei dati personali nella giurisprudenza della Corte europea dei diritti dell'uomo: brevi riflessioni introduttive

DI GILBERTO FELICI*

SOMMARIO: 1. La definizione di «dati personali». – 2. Il diritto alla "protezione dei dati personali" e la nozione di "vita privata e familiare" ai sensi dell'articolo 8 CEDU. – 3. Gli elementi presi in considerazione dalla Corte europea per forgiare la nozione di "vita privata e familiare" riguardo alla protezione dei dati personali. – 4. Il test di convenzionalità nell'ambito della tutela dei dati personali. – 5. Casi recenti.

1. La definizione di «dati personali»

La protezione dei dati personali gioca un ruolo fondamentale nell'esercizio del diritto al rispetto della vita privata e familiare consacrato dall'articolo 8 della Convenzione europea dei diritti dell'uomo (*Satakunnan Markkinaporsi Oy e Satamedia Oy c. Finlandia*, § 133).

E' importante precisare che tanto nell'ambito del diritto dell'Unione Europea quanto in quello della *soft law* elaborata dal Consiglio d'Europa, qualsiasi informazione può essere ritenuta un "dato personale" purché si riferisca a una persona identificata o identificabile. I "dati personali", infatti, sono informazioni che riguardano una persona la cui identità è manifestamente chiara o può in ogni caso essere accertata mediante l'ottenimento d'informazioni supplementari.

La nozione di "dati personali", inoltre, ingloba non soltanto quelle informazioni concernenti la vita privata di una persona – comprese le sue attività professionali – ma anche, in determinate condizioni (cfr. *infra*), le informazioni sulla sua vita pubblica.

A ciò si aggiunga che, sebbene tanto la normativa dell'Unione Europea in materia di protezione dei dati, quanto la Convenzione 108 elaborata dal Consiglio d'Europa facciano riferimento esplicito alla tutela dei dati personali delle sole persone fisiche, in realtà anche le persone giuridiche godono di certe tutele nel trattamento dei propri dati personali, grazie alla giurisprudenza elaborata dalla Corte europea dei diritti dell'uomo. Numerose sentenze della Corte di Strasburgo, infatti, riguardano ricorsi presentati da persone giuridiche relativi a violazioni del loro diritto alla protezione contro l'uso dei loro dati personali *ex* articolo 8 della Convenzione.

* Giudice della Corte europea dei diritti dell'Uomo.

Risulta dunque fin da subito evidente l'importanza del *case-law approach* della Corte europea dei diritti dell'uomo che, proprio nell'ambito dell'articolo 8 della Convenzione, con la sua giurisprudenza ha adottato un'interpretazione evolutiva della Convenzione europea dei diritti dell'uomo fino a renderla un vero e proprio *living instrument*. Com'è ben noto, infatti, il diritto alla protezione dei dati personali non è esplicitamente previsto nel testo della Convenzione, in quanto quest'ultima – elaborata nel 1949 – si limita a evocare testualmente, nell'articolo 8, il diritto alla protezione della vita privata e familiare di ogni individuo.

È proprio grazie alla giurisprudenza della Corte europea che si è, infatti, affermato un diritto alla protezione dei dati personali, facendo discendere quest'ultimo dal diritto alla protezione della vita privata e familiare di cui all'articolo 8 (che costituisce, tra tutte le disposizioni convenzionali, probabilmente quella maggiormente interessata da procedimenti di interpretazione evolutiva).

Oltre alla giurisprudenza evolutiva della Corte di Strasburgo, la "Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale" (più comunemente conosciuta sotto il nome di "Convenzione 108") del Consiglio d'Europa si configura quale pietra angolare della protezione dei dati personali delle persone. Aperta alle firme nel 1981 e in seguito entrata in vigore nel 1985, la Convenzione 108 rappresenta il primo strumento internazionale obbligatorio: (i) avente per scopo la protezione delle persone contro l'uso abusivo del trattamento automatizzato dei dati di carattere personale; e (ii) di disciplina del flusso transfrontaliero dei dati.

Sebbene ormai superata dalle recenti evoluzioni tecnologiche, la Convenzione 108 rimane ancora oggi importante per la sua impostazione e per i principi di base da essa enunciati: oltre le garanzie previste per il trattamento automatizzato dei dati di carattere personale, essa bandisce il trattamento dei dati "delicati" sull'origine razziale, sulle opinioni politiche, la salute, la religione, la vita sessuale e le condanne penali, se in assenza di garanzie previste dal diritto interno. La Convenzione garantisce, inoltre, il diritto delle persone di conoscere le informazioni catalogate su di loro e a esigere – se del caso – delle rettifiche, con la sola eccezione dei casi in cui sia presente un interesse maggiore (quali la sicurezza pubblica e la difesa), e impone delle limitazioni ai flussi transfrontalieri di dati negli Stati in cui non esista alcuna protezione equivalente.

2. Il diritto alla "protezione dei dati personali" e la nozione di "vita privata e familiare" ai sensi dell'articolo 8 CEDU

La protezione dei dati personali rientra ormai, grazie alla giurisprudenza della Corte di Strasburgo, nell'ambito del diritto al rispetto della vita privata e familiare di cui all'articolo 8 della Convenzione europea, che è una norma paradigmatica.

Ai sensi del § 1 dell'articolo 8 ("*diritto alla vita privata e familiare*"), infatti:

"1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza".

L'incorporazione del diritto alla protezione dei dati personali nell'ambito dell'articolo 8 della Convenzione trova un suo fondamento nella circostanza per cui la raccolta, la memorizzazione, la conservazione e la divulgazione da parte dello Stato d'informazioni e dati riguardanti la vita privata di un individuo, risultano di per sé sufficienti ad interferire con il diritto di quest'ultimo al rispetto della sua vita privata, costituendo dunque un'ingerenza nel senso tipico convenzionale[1], a nulla rilevando che le informazioni memorizzate siano o meno utilizzate in seguito[2].

Una tale ingerenza risulta peraltro particolarmente forte ed evidente soprattutto laddove i dati e le informazioni raccolte, conservate e divulgate riguardino il passato lontano di un individuo[3], o qualora ne rivelino le opinioni politiche, rientrando così in quelle categorie particolari di dati che richiedono una protezione rinforzata[4].

In quali termini i dati e le informazioni personali possano rientrare nella nozione di "vita privata e familiare"?

A questo proposito, si rileva che i giudici di Strasburgo hanno negli anni stabilito che l'articolo 8 della Convenzione trova ad applicarsi in molteplici casi, quali: l'ottenimento e la conservazione da parte dei servizi di sicurezza o di altri organi dello Stato di *dossiers* o di dati a carattere personale o di natura pubblica (ad esempio, le informazioni relative all'attività politica di un individuo[5]); la raccolta dei dati personali durante i censimenti ufficiali[6] la presa di impronte digitali e di fotografie da parte della polizia[7]; la raccolta e la conservazione di campioni cellulari e profili di DNA[8] (in particolare, l'assenza di garanzie nell'ambito della raccolta, conservazione e cancellamento delle impronte digitali di persone sospettate di aver commesso delle infrazioni, ma poi non condannate[9]); la raccolta di dati medico-sanitari, così come la conservazione di cartelle cliniche[10]; l'iscrizione del nome di una persona in un archivio giudiziario nazionale relativo agli autori di infrazioni sessuali[11], o ancora la raccolta e memorizzazione di dati GPS[12] e, nel caso di sportivi di alto livello costretti dallo Stato – nell'ambito della lotta contro il doping

[1] *Leander c. Svezia; Amann c. Svizzera; S. e Marper c. Regno Unito.*
In particolare *S. e Marper c. Regno Unito, 4 dicembre 2008, § 67: « Le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 [de la Convention européenne des droits de l'homme qui garantit le droit au respect de la vie privée et familiale, du domicile et de la correspondance](…). Peu importe que les informations mémorisées soient ou non utilisées par la suite ».*
[2] *Amann c. Svizzera §§ 65-67; Leander c. Svezia § 48; Kopp c. Svezia § 53.*
[3] *Rotaru c. Romania, §§ 43-44.*
[4] *Catt c. Regno Unito, §§ 122 e 123.*
[5] Si vedano*, inter alia, Rotaru c. Romania §§ 43-44; Associazione "21 dicembre 1989" e altri c. Romania § 115; Catt c. Regno Unito, §93.*
[6] *X c. Regno Unito, n. 9702/82.*
[7] *Murray c. Regno Unito; McVeigh, O' Neill e Evans c. Regno Unito; S. e Marper c. Regno Unito e MK c. Francia.*
[8] *Van der Velden c. Olanda; S e Marper c. Regno Unito.*
[9] *M. K c. Francia, § 26.*
[10] *Chave née Jullien c. Francia.*
[11] *Gardel c. Francia § 58.*
[12] *Uzun c. Germania.*

– a comunicare per il trimestre a venire la loro agenda quotidiana dettagliata, weekend compreso, e a segnalare ogni modifica apportata a tale agenda[13].

Come già anticipato al § 1 che precede, peraltro, anche le informazioni pubbliche possono rientrare nel campo di applicazione della nozione di "vita privata" qualora sistematicamente raccolte e conservate dalle autorità in appositi archivi. In materia di protezione dei dati personali, dunque, il fatto che le informazioni in causa siano già di dominio pubblico non le sottrae necessariamente alla protezione garantita dall'articolo 8 della Convenzione[14].

Nella sentenza *Satakunnan Markkinaporsi Oy e Satamedia Oy c. Finlandia*, infatti, la Corte precisa che le considerazioni legate alla vita privata entrano in gioco nei casi in cui le informazioni e dati a carattere personale siano stati: *1)* raccolti su una persona ben precisa; *2)* trattati o utilizzati; *3)* resi pubblici in un modo o in una misura superiore rispetto a quella che l'interessato avrebbe potuto legittimamente attendersi (§ 136)[15].

A titolo di esempio, la Corte ha più volte affermato che il semplice fatto che le autorità dello Stato catturino delle fotografie in aree pubbliche generalmente non costituisce una interferenza con il godimento del diritto alla vita privata, ma quest'ultima si configurerà qualora l'immagine sia registrata o utilizzata[16].

3. Gli elementi presi in considerazione dalla Corte europea per forgiare la nozione di "vita privata e familiare" riguardo alla protezione dei dati personali

Al fine di determinare se le informazioni a carattere personale conservate dalle autorità siano in grado di far entrare in gioco un aspetto della vita privata dell'interessato, la Corte tiene conto di alcuni elementi[17], quali: *(i)* il contesto specifico nell'ambito del quale i dati e le informazioni sono stati raccolti e conservati; *(ii)* la loro natura; *(iii)* le modalità della loro utilizzazione e trattamento, oltre che i risultati che ne possono essere tratti.

Con riferimento alla natura dei dati personali e al contesto specifico in cui questi sono raccolti e conservati, la Corte – in casi riguardanti persone sospettate di terrorismo – ha ad esempio ritenuto che: *a)* consegnando e conservando i dati personali di base riguardanti la persona arrestata – o altre persone presenti al momento e sul luogo

[13] *Fédération nationale des associations et syndacats des sportifs e altri c. Francia §§ 155-159*.
[14] *Satakunnan Markkinaporsi Oy e Satamedia Oy c. Finlandia*, *§ 134.*
[15] Nel caso citato, la Corte ha affermato che i dati raccolti, trattati e pubblicati dai giornali – che davano delle precisioni sui redditi imponibili provenienti dal lavoro e da altre fonti, cosi come sul patrimonio netto imponibile di numerose persone – rilevavano chiaramente della vita privata di queste ultime, indipendentemente dal fatto che, ai sensi del diritto finlandese, il pubblico avesse la possibilità di accedere a tali dati seguendo determinate regole *(§ 137*).
[16] *Peck c. Regno Unito*; *Perry c. Regno Unito*; *Khmel c. Russia*.
[17] *S. e Marper c. Regno Unito*, *4 dicembre* 2008, § 67 : *« Toutefois, pour déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu [un aspect] de la vie privée (...) la Cour tiendra dument compte du contexte particulier dans lequel ces informations ont été recueillies être conservées, de la nature des données consignées, de la manière dont elles sont utilisées et traitées et des résultats qui peuvent en être tirés».*

dell'arresto – le autorità competenti non superano i limiti legittimi dei procedimenti penali relativi alle infrazioni terroristiche[18]; e *b)* in ogni caso, in tali situazioni, lo Stato gode di un margine di apprezzamento più ampio, specialmente per quanto riguarda la conservazione di informazioni su persone che erano state nel passato implicate in attività terroristiche[19]. La Corte è, infatti, solita prendere in conto la natura delle informazioni in questione per determinare il margine di apprezzamento dello Stato[20].

Con riferimento poi alle modalità di utilizzazione e trattamento dei dati personali, oltre che ai risultati che ne possono essere tratti, la Corte europea ha ad esempio rilevato come un profilo di DNA contenga una quantità importante di dati a carattere personale unici[21]. Similmente, al § 51 della sentenza *M. N. e altri c. San Marino*, i giudici di Strasburgo hanno precisato che anche le informazioni ottenute dai documenti bancari costituiscono dei dati personali, poco importa che si tratti d'informazioni sensibili di un individuo o relative a sue attività professionali.

4. Il test di convenzionalità nell'ambito della tutela dei dati personali

Dopo aver ribadito il contenuto del § 1 dell'articolo 8, occorre altresì porre l'accento sul successivo § 2, ai sensi del quale:

"2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui".

Come per le altre interferenze di cui all'articolo 8 della Convenzione, affinché la raccolta, la memorizzazione, la conservazione e la divulgazione da parte dello Stato d'informazioni e dati riguardanti la vita privata di un individuo sia conforme al requisito della legalità, è innanzitutto necessario che la legislazione nazionale: *(i)* sia adeguatamente accessibile e prevedibile; e *(ii)* assicuri di impedire un'utilizzazione dei dati personali non conforme alle garanzie previste all'articolo 8 della Convenzione[22].

Nella già citata sentenza *S e Marper c. Regno Unito* (relativa alla registrazione di dati biometrici) la Corte ha, infatti, spiegato che per rispettare il criterio della legalità è

[18] *Murray c. Regno Unito*, *§ 93*.
[19] *Segerstedt-Wiberg e altri contro Svezia*, *§ 88*.
[20] *G.S.B. c. Svizzera*, *§ 93*.
[21] *S. e Marper c. Regno Unito*, *§ 75*.
[22] Si veda la sentenza *Dimitrov-Kazakov c. Bulgaria, § 32*, ai sensi della quale*:* «*Pour ne pas enfreindre l'article 8, une telle ingérence doit avoir été « prévue par la loi », poursuivre un but légitime au regard du paragraphe 2 et, de surcroît, être nécessaire dans une société démocratique pour atteindre ce but* (…)*. Il faut d'abord que la « loi » soit suffisamment accessible : le citoyen doit pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné. La loi doit ensuite être énoncée avec assez de précision pour permettre à l'individu de régler sa conduite, en s'entourant au besoin de conseils éclairés (...)*».

necessaria l'esistenza di norme chiare e dettagliate che disciplinino le finalità e l'applicazione delle misure in questione, oltre che di garanzie minime relative, quali – *inter alia* – la durata; la conservazione; l'utilizzazione; l'accesso ai terzi; le procedure per preservare l'integralità e la confidenzialità dei dati; così come le procedure per la loro distruzione, in modo da evitare rischi di abuso e di arbitrarietà. Nel caso di specie, tuttavia, avendo la Corte concluso per una violazione a causa dell'evidente mancanza di proporzionalità degli ampi poteri di conservazione dei dati personali, la stessa non si è dunque pronunciata sulla conformità della legislazione interna ai requisiti di legalità sopra menzionati.

Al contrario, la legalità ha assunto un ruolo decisivo nel già citato caso *M.M. c. Regno Unito*. La Corte, da un lato, ha riconosciuto che vi potesse essere la necessità di registrare in modo completo i precedenti giudiziari. Dall'altro, ha poi indicato *(§ 199*) che una conservazione indifferenziata e incondizionata di dati relativi a dei precedenti giudiziari sarebbe stata difficilmente conforme alle esigenze di cui all'articolo 8. Quanto precede, soprattutto in assenza di disposizioni normative chiare e dettagliate atte a specificare le garanzie applicabili, e a dettare o recepire la disciplina riguardo alle circostanze in cui i dati possono essere raccolti; al la durata della loro conservazione all'utilizzazione che ne può essere fatta; alle circostanze nelle quali tali dati e informazioni possono essere distrutti. In tal caso, dunque, la Corte ha concluso per una violazione dell'articolo 8 della Convenzione per l'assenza di sufficienti garanzie.

In altri casi, invece, l'esame della Corte si è focalizzato sulla necessità delle misure di ingerenza.

Nella già citata sentenza *S. e Marper c. Regno Unito* (§ 112), ad esempio, i giudici di Strasburgo hanno affermato che la protezione offerta dall'articolo 8 sarebbe affievolita in maniera inaccettabile se l'uso di moderne tecniche scientifiche nel sistema della giustizia penale fosse autorizzato ad ogni costo e comunque, senza un attento bilanciamento dei vantaggi che potrebbero derivare da un ampio ricorso a tali tecniche *da una parte* e degli interessi fondamentali relativi alla protezione della vita privata, *dall'altra.*

Al contrario, nel caso *Leander c. Svezia,* la Corte ha riconosciuto la necessità di raccogliere e conservare informazioni personali segrete a cui ricorrere nel determinare l'idoneità dei candidati a cariche importanti per la sicurezza nazionale. Nel concludere per una non violazione dell'articolo 8, la Corte ha infatti riconosciuto che l'esistenza di molteplici misure di controllo da parte di organismi indipendenti rispetto al Governo rappresentasse una salvaguardia sufficiente contro eventuali abusi. Similmente, in *GSB c. Svizzera*, la rivelazione da parte di una banca svizzera d'informazioni bancarie alle autorità fiscali statunitensi non è stata ritenuta disproporzionata, considerata la natura strettamente finanziaria delle informazioni in questione e l'esistenza di garanzie.

5. Casi recenti

Per comprendere a pieno la protezione e la tutela accordata dai giudici di Strasburgo in ambito di dati personali si può accennare anche ad alcuni casi recenti trattati dalla Corte.

A) La giurisprudenza consolidata della Corte europea dei diritti dell'uomo.

La giurisprudenza ormai consolidata della Corte europea può essere analizzata tramite lo studio più nel dettaglio di due giudicati: il primo (*Catt c. Regno Unito*) nell'ambito della quale i giudici di Strasburgo hanno concluso per una violazione dell'articolo 8; e il secondo (*Murray c. Regno Unito*) in cui si è invece concluso per una non violazione:

– ***Catt c. Regno Unito*** (24 gennaio 2019)

Nel 2005 il ricorrente – che da numerosissimi anni militava attivamente presso movimenti pacifisti – iniziò a partecipare ad alcune manifestazioni organizzate da un gruppo violento di attivisti, durante le quali si rese necessaria la presenza della polizia. In tale contesto, varie informazioni personali – quali il suo nome, il suo indirizzo, la sua data di nascita, ma anche l'indicazione delle manifestazioni a cui aveva preso parte (la maggior parte delle quali riguardavano la sua partecipazione alle manifestazioni organizzate dal gruppo violento di attivisti, ma anche a delle riunioni politiche o sindacali) – vennero raccolte e conservate in un database della polizia relativo all'estremismo ("*Extremism database"*). Il ricorrente si rivolse dunque alle autorità nazionali per ottenere la soppressione di tali informazioni dall'*Extremism database.*

Con riferimento alla raccolta da parte della polizia dei dati personali del ricorrente, la Corte riconosce che la stessa è avvenuta in modo trasparente ed è stata giustificata dall'esigenza imperativa di sorvegliare le manifestazioni organizzate da gruppi riconosciuti come violenti e potenzialmente criminali.

La conservazione di tali dati, invece, non risulta rispondere ad un bisogno imperioso, non essendo stato in alcun modo dimostrato che la conservazione di dati relativi al ricorrente – specialmente quelli relativi alla sua partecipazione a delle manifestazioni pacifiche – rivestisse un carattere assolutamente necessario, né che rispondesse ai bisogni di un'inchiesta particolare.

Più precisamente, la Corte nota innanzitutto l'assenza di norme volte a disciplinare la durata massima di conservazione di tali dati, con la conseguenza che questi ultimi sarebbero potuti essere conservati illimitatamente nel tempo. Se anche, infatti, il ricorrente poteva (come ha fatto) chiedere la comunicazione e l'eliminazione di tali informazioni dal database, in ogni caso tale garanzia si è rivelata molto debole, avendo le autorità opposto un rifiuto alla richiesta di eliminazione delle informazioni relative al ricorrente o di motivare la decisione relativa alla loro conservazione.

A tali considerazioni, la Corte aggiunge altresì che la polizia non risulta aver rispettato la definizione di "database relativo all'estremismo" dalla stessa delineata, avendo infatti conservato anche dati personali relativi alla partecipazione del ricorrente a manifestazioni politiche e sindacali pacifiche.

Nel caso di specie, la Corte ha dunque concluso per una violazione dell'articolo 8 della Convenzione, considerando che l'eliminazione di dati personali da un database non sia un compito di una complessità eccessiva e che sarebbe totalmente contrario alla necessità di proteggere il diritto alla vita privata accettare che uno Stato possa invocare il modo in cui un determinato database è stato elaborato (in particolare la difficoltà di accesso ai dati e di una loro eventuale modifica), per giustificare il rifiuto di eliminare le informazioni in esso contenute.

– ***Murray c. Regno Unito*** (28 ottobre 1994)

Il caso di specie riguarda l'arresto e la reclusione in Irlanda del Nord di un soggetto sospettato di terrorismo. In tale contesto, le autorità nazionali hanno adottato varie misure (penetrazione nell'abitazione e perquisizione; consegna e conservazione di informazioni personali, ivi compresa una fotografia della prima ricorrente) costituenti una vera e propria ingerenza ai sensi dell'articolo 8 della Convenzione.

La Corte ha però concluso, in questo caso, che una tale ingerenza non avesse comportato una violazione del diritto al rispetto della vita privata di cui all'articolo 8 della Convenzione.

Più precisamente, i giudici di Strasburgo hanno precisato che ogni misura presa dalle autorità: (i) aveva una sua base in diritto interno risultando così "prevista dalla legge"; (ii) perseguiva uno scopo legittimo consistente nella prevenzione di infrazioni di carattere terroristico; e infine (iii) risultava essere necessaria in una società democratica e non sproporzionata rispetto al fine perseguito, rappresentando infatti un giusto equilibrio tra il diritto di ogni individuo al rispetto della propria vita privata e la necessità dello Stato di prendere delle misure efficaci per prevenire la criminalità terroristica.

B) <u>I casi ancora pendenti davanti alla Grande Camera.</u>

Due casi– piuttosto complessi e tra loro riuniti – sono tuttora pendenti dinanzi alla Grande Camera che, come noto, rappresenta la formazione giudiziaria che esprime la giurisprudenza della Corte al livello più elevato.

– ***Big Brother Watch e altri c. Regno Unito*** (13 settembre 2018)

Il caso riguarda la conformità alla Convenzione di programmi di sorveglianza segreta che attuano un'intercettazione massiccia di comunicazioni esterne.

I ricorrenti (imprese, organismi caritativi, organizzazioni e singoli individui) lamentano l'ampia portata – a loro dire non compatibile con l'articolo 8 della Convenzione – di tre programmi di sorveglianza adottati dal Governo britannico:

1. il programma d'intercettazione massiccia delle comunicazioni autorizzato dall'art. 8 § 4 della legge sulla *Regulation of Investigatory Powers Act* (la "RIPA");
2. il programma di condivisione delle informazioni ottenute dall'intelligence; e
3. il programma di acquisizione dei dati di comunicazione previsto dal capitolo II della RIPA.

Con sentenza del 13 settembre 2018, la I Sezione della Corte europea ha concluso per la:

a) violazione degli articoli 8 e 10 quanto al programma di cui all'art. 8 § 4 della RIPA, perché regolato da disposizioni non conformi al requisito di "qualità della legge" e non in grado di limitare l'ingerenza a quanto strettamente "necessario in una società democratica";

b) non violazione dell'articolo 8 con riferimento al programma di condivisione delle informazioni ottenute dall'intelligence, poiché nella specie nulla dimostrava la presenza di gravi carenze nella messa in opera o nel funzionamento del programma; e

4. violazione degli articoli 8 e 10 per quanto riguarda il programma di acquisizione dei dati di comunicazione previsto dal capitolo II della RIPA, essendo questo privo di base legale.

Come già anticipato, il 4 febbraio 2019, il caso è stato rinviato – su domanda della ricorrente – dinanzi alla Grande Camera, dove è tuttora pendente.

– ***Centrum för rättvisa c. Svezia*** (18 giugno 2019)

Il caso riguarda la proporzionalità e le garanzie offerte dalla legislazione svedese in materia di spionaggio di segnali elettromagnetici.

La ricorrente nel caso di specie è un'organizzazione svedese a scopo non lucrativo che, nei litigi contro lo Stato, rappresenta i propri clienti che si ritengono vittime di una violazione dei loro diritti e libertà derivanti dalla Convenzione e dal diritto svedese. Tenuto conto della natura delle proprie funzioni di organizzazione non governativa che controlla l'attività di molteplici attori statali, la ricorrente ritiene che vi sia il rischio che le proprie comunicazioni avvenute per telefonia mobile siano stati (o saranno in futuro) intercettate ed esaminate dall'attività di spionaggio di segnali elettromagnetici.

Con sentenza del 19 giungo 2018, la III Sezione della Corte – dopo aver analizzato vari elementi (la portata delle misure di spionaggio; la loro durata; il loro sistema di autorizzazione; i procedimenti da seguire per la conservazione, la consultazione, l'esame, l'utilizzazione e la distruzione dei dati intercettati; le condizioni nelle quali questi ultimi possono essere comunicati ai terzi; il controllo dell'applicazione di tali misure; la loro notifica e i ricorsi disponibili) – ha concluso all'unanimità per la non violazione dell'articolo 8 della Convenzione.

La Corte, infatti, ha ritenuto che – benché siano possibili dei miglioramenti – il sistema svedese di spionaggio di segnali elettromagnetici, se esaminato in astratto, non fa apparire gravi carenze nella sua struttura o funzionamento; risulta proporzionato al fine perseguito; e offre garanzie adeguate e sufficienti contro rischi di abuso e arbitrarietà.

The General Data Protection Regulation (GDPR) and the current review of E-Privacy Directive in a new EP Regulation for personal data

DI ANDREAS SCHWAB *

1. Introduction

In this Digital age we are living, a key role is played by data: data collection, data access, data ownership and data exploitation have transformed the economy and society, affecting the daily lives of all European citizens and all sectors of activity within the Internal market by bringing enormous benefits. It might be considered as the fifth fundamental freedom. The way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules. Citizens need to trust and embrace data use only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules. In this context, from the beginning, our priorities within the European Parliament, as representatives of all European citizens, were to ensure the creation of an appropriate regulatory environment for the adoption of an effective data policy in the digital single market.

2. The steps forward in this direction: an overview of the legislative process within the European Institutions

Over the last few years, the European Parliament together with the European Commission and the Council worked very hard on the protection of personal data and respect for private life inasmuch they are important fundamental human rights.

We have always insisted on the need to find a balance between enhancing security and safeguarding human rights, including data protection and privacy. Therefore it were important to provide new EU data protection rules strengthening citizens' rights and simplifying rules for companies in the digital age.

Article 16 of the Treaty on the Functioning of the European Union (TFEU) and articles 7 and 8 of the EU Charter of Fundamental Rights provided the legal basis for the legislation in this matter.

* Membro del Parlamento europeo, Commissione Mercato Interno e Protezione dei Consumatori

2.1. The General Data Protection Regulation (GDPR)

The first EU Data Protection Reform was presented in January 2012 by the European Commission to make Europe fit for the digital age. It aimed to give all European citizens the same data protection rights across the EU – and regardless of where their data is processed.

Then, on December 2015, an agreement was reached on the new data protection rules, establishing a modern and harmonised data protection framework across the EU. The agreement was also a major step forward in the implementation of the Digital single market (DSM) strategy.

In this context, a regulation and a directive were adopted:

1) The General Data Protection Regulation (GDPR) (EU 2016/679) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. It came into force on 24 May 2016 and was applied across the EU from 25 May 2018.

With these rules we aimed to protect all EU citizens from privacy and data breaches by creating at the same time a clearer and more consistent framework for businesses.

Between the rights enjoyed by citizens there are included: i) a clear and affirmative consent for their data to be processed and the right to receive clear and understandable information about it; ii) the right to be forgotten: a citizen can ask for his/her data to be deleted; the right to transfer data to another service provider; iii) the right to know when data has been hacked.

One of the new features of this Regulation is that the rules are applied to all companies operating in the EU, even if these companies are based outside it. Moreover, it is possible to impose corrective measures, such as warnings and orders, or fines on firms that break the rules.

However, there are still some issues related to the enforcement of this Regulation. Indeed, in each member states the application of the Regulation is left to the national Data Protection Authorities: this means that its interpretation is not harmonised across the EU. In this respect, it is necessary to build a better legal network to enforce the regulation in a consistent manner within the single market.

2) the Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data. It entered into force on 5 May 2016 and EU countries transposed it into their national law by 6 May 2018. With this directive, we wanted to guarantee the citizens' fundamental right to data protection whenever personal data is used by law enforcement authorities. It ensures that the personal data of victims, witnesses, and suspects of crime are duly protected and facilitates cross-border cooperation in the fight against crime and terrorism.

2.2 Current review of E-Privacy Directive in a new EP Regulation (for personal data)

Last but not least, within the Strategy for the Digital Single Market, the current e-Privacy Directive (Directive 2002/58/EC) - the processing of personal data and the protection of privacy in the electronic communications sector - is now subjected to a review to ensure that its requirements were in line with those of the GDPR.

On January 2017 indeed, the Commission presented its draft proposal for a Regulation which will repeal the current e-Privacy Directive. The Regulation's goal is to get a coherent and up-to-date framework capable to strike the balance between industry's interests (ensuring free movement of data and e-communications services within the EU) and users' rights to privacy and data protection.

The legislative process for the time being is blocked, because a consensus between Member states in the Council is still not reached.

3. Conclusion

In conclusion, the protection of data is one of the main pillars of the Digital Single Market (DSM) Strategy, and therefore it is also necessary to guarantee its free and safe movement within the European Union.

We strong believe that the EU can become a leading role model for the modern society that nowadays relay on the use of data for everything. In order to fulfil this ambition, it needs to build on a strong regulatory and legal framework – in terms of data protection, fundamental rights, safety and cybersecurity.

In this context, we worked and are still working to ensure consistency between the different legal instruments addressing personal data in this new digital environment, with the objective to increase trust in and the security of data for all the European citizens.

Garantire la protezione dei diritti fondamentali nel mercato unico digitale: verso un approccio sinergico tra il diritto della concorrenza e la protezione dei dati

DI ANNA COLAPS *

1. Introduzione

Il presente contributo si propone di analizzare un aspetto specifico della protezione dei dati personali nel mercato unico digitale, quello della sua relazione con il diritto della concorrenza[1].

La tesi di fondo è che una maggiore sinergia tra la disciplina in materia di protezione dei dati ed il diritto della concorrenza possa contribuire all'integrazione europea,

* Esperto legale e membro di gabinetto del Garante europeo della protezione dei dati. Dottore di ricerca in diritto dell'Unione europea presso l'Università degli studi di Napoli "Parthenope". Le opinioni espresse in questo scritto sono personali e non riflettono necessariamente la posizione dell'Istituzione.

[1] Entrambe le discipline intendono servire (anche) gli scopi del mercato interno e del mercato unico digitale. In particolare, la disciplina di protezione dei dati, sostanziata prima nella Direttiva 1995/46/CE e poi nel Regolamento (UE) n. 679/2016 (da qui in avanti, GDPR), riposa (anche) sugli obiettivi del mercato interno. Il GDPR si propone il duplice obiettivo di garantire un livello coerente ed elevato di protezione delle persone fisiche e di rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione. Il consolidamento del quadro normativo di riferimento fu inteso come necessario per creare il clima di fiducia tale da consentire lo sviluppo dell'economia digitale nel mercato interno. La disciplina in materia di protezione dei dati è dunque anche strumento di integrazione positiva dei mercati.
La dottrina specialistica aveva affrontato da diversi anni la questione dell'interazione tra le due discipline e della rilevanza del controllo dei dati personali per le dinamiche competitive del mercato interno. Il tema della relazione tra le due discipline è poi giunto anche all'attenzione dei *policy maker*.

pienamente fondata sul rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani[2].

Una nota metodologica si impone sin da subito: all'interno dell'ampio contesto dell'economia digitale, oggetto dell'analisi saranno i mercati nei quali i dati personali rappresentano l'input fondamentale dell'attività[3].

In primo luogo, lo scritto analizza i trend nei mercati di riferimento, in termini di modello di business prevalente, pratiche abusive di sfruttamento e accresciuti livelli di concentrazione dei mercati, fornendo al lettore una rappresentazione dello stato delle principali problematiche di natura competitiva dei mercati digitali.

In secondo luogo, il contributo offre una lettura dei costi diversi da quelli economici, in particolare il costo democratico, che la nostra società sopporta in conseguenza dei trend di mercato prevalenti.

In terzo luogo, lo scritto analizza la nozione di responsabilità speciale nel diritto della concorrenza in chiave comparata con la nozione di responsabilità e l'approccio basato sul rischio nella disciplina di protezione dei dati. Tali considerazioni sono volte a dimostrare che entrambe le discipline presentano importanti elementi che consentono un'applicazione rinforzata rispetto a quelle pratiche che presentano maggiori rischi sistemici per gli individui e l'innovazione.

In quarto luogo, il contributo avanza proposte di teorie del danno concorrenziale nuove, che consentano di integrare i diritti fondamentali all'interno della comprensione dei mercati digitali.

Lo scritto conclude nel senso che occorre ed è possibile realizzare un'integrazione positiva tra le due discipline, che si basi propriamente e compiutamente sul rispetto dei diritti fondamentali.

2. Analisi delle tendenze di mercato prevalenti

Nei mercati nei quali i dati personali rappresentano l'input fondamentale dell'attività prevale un modello di business basato sul monitoraggio persistente degli utenti, la cui dimensione ed estensione resta prevalentemente sconosciuta agli interessati. Questo modello è in grado di produrre anche effetti manipolativi perché spinge gli individui a compiere scelte non efficaci sotto il profilo della tutela dei diritti fondamentali alla protezione dei dati e alla riservatezza. Livelli elevati di concentrazione dei mercati e la presenza di conglomerati amplificano queste caratteristiche dell'ecosistema digitale.

2.1. Modello di business

[2] Art. 2, Trattato sull'Unione europea (TUE).

[3] Cd. *Data-driven markets*, nei quali spesso il consumatore non paga un prezzo monetario. J. M. NEWMAN, *Antitrust in zero-price markets: foundations*, in *University of Pennsylvania Law Review*, 2015. Tali mercati hanno formato oggetto di una disamina completa nella tesi di dottorato dell'autore di questo contributo, A. Colaps, Complying with EU data protection law in data-driven markets: an assessment as an either entry barrier or a competitive advantage, 2016.

L'economia digitale si basa sullo sfruttamento intensivo dei dati personali, che rappresentano un input fondamentale in un crescente numero di settori[4]. Nell'ultimo decennio, l'approvvigionamento dei dati personali è sfociato in monitoraggio persistente delle vite degli individui.

Il tipo di monitoraggio che il presente contributo analizza è quello reso possibile dal cd. tracciamento (o tracking), che è alla base dell'offerta di molteplici prodotti e servizi: social media, commercio elettronico, applicazioni di fitness, applicazioni sulla salubrità dell'aria, piattaforme di streaming musicale, servizi di video-conferenza[5]. La lista è, in realtà, potenzialmente illimitata[6]. Il tracciamento, combinato con ampie capacità di analisi dei dati ed elementi di psicologia comportamentale, consente ad alcuni attori del mercato di predire con grande accuratezza la propensione dei consumatori verso un bene o servizio. I dati raccolti attraverso il tracciamento includono dati personali, quali ad esempio, quelli sulla posizione geografica, o categorie speciali di dati, quali quelli idonei a rivelare lo stato di salute[7].

In particolare, l'ecosistema ad-tech (da advertising technology) è oggetto di un numero crescente di analisi e studi[8]. Nell'epoca dell'Internet of everything, di quasi totale interconnessione e sincronizzazione tra dispositivi tecnologici, vale la pena di sottolineare, con approccio empirico, il ruolo che gli unique identifier, assegnati agli individui senza la loro conoscenza o consapevolezza, svolgono nell'economia basata sulla sorveglianza commerciale[9]. Studi empirici hanno dimostrato che tali identificatori permanenti, ai quali sono collegati informazioni di ogni sorta, sono utilizzati per tracciare gli utenti attraverso servizi e dispositivi, di modo da consentire di creare dei profili completi sull'individuo stesso indipendentemente dal dispositivo utilizzato ed indipendentemente dal servizio di cui si fruisce[10]. Gli identificatori in esame rappresentano essi stessi stati dati personali, ai sensi del GDPR, in quanto consentono di rivelare l'identità dell'individuo che utilizza il dispositivo[11]. All'utente resta sconosciuta

[4] A. COLAPS, *Big Data: Is EU Competition Law Ripe Enough to Meet the Challenge?* in R. MASTROIANNI, A. ARENA (a cura di), *60 Years of EU Competition Law: Stocktaking and Future Prospects*, Napoli, 2017, p. 31 ss.

[5] Rileva, in questo contesto, anche la Direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche (cd. ePrivacy). Si veda anche: Comitato europeo per la protezione dei dati, Parere 5/2019 sulla relazione tra la direttiva ePrivacy e il GDPR, marzo 2109.

[6] La tracciabilità per scopi diversi da quelli commerciali o politici resta fuori dalle finalità del contributo.

[7] Il trattamento di categorie particolari di dati è, in linea di principio, vietato dalla normativa europea. In deroga alla regola generale, sono previste eccezioni per casi precisi e delimitati (art. 9 GDPR).

[8] Fra tutti, si veda: Information Commissioner's Office (UK), Update report into adtech and real time bidding, giugno 2019.

[9] Forbrukerradet, Out of control, How consumers are exploited in the online advertising industry, gennaio 2020.

[10] Forbrukerradet, Out of Control, Technical report, A review of data sharing by popular mobile apps, gennaio 2020. La sincronizzazione è resa possibile dall'*ID syncing*.

[11] Art. 4(1) lett. a), GDPR.

l'intera rete di ulteriori operatori che operano nel mercato[12], oltre la dimensione e l'estensione stressa del tracciamento[13].

Quella per l'accaparramento dei dati personali è una competizione decisiva perché rappresenta la porta di ingresso per conoscere abitudini, preferenze, desideri e timori degli individui, e dunque adattare l'offerta commerciale rispetto a tali parametri. Ad esempio, il tracciamento può essere veicolo per una discriminazione dei prezzi di primo grado (cd. first-degree price discrimination), in virtù della quale l'operatore riesce ad imporre un prezzo diverso per ciascun consumatore, fissandolo al livello massimo che il consumatore è disposto a pagare per il bene o servizio (cd. reservation price)[14].

Lo sfruttamento dei dati personali non ha solo una sola valenza commerciale ed economica, ma importanti sono le ripercussioni sia a livello individuale che collettivo. L'ecosistema digitale è attraversato da tentativi di manipolazione delle scelte personali e indirizzamento dell'opinione pubblica, ad esempio in materia di elettorato attivo[15]. Inoltre, la semplice possibilità di essere sottoposti a sorveglianza online è in grado di dissuadere gli individui dallo svolgimento di attività o dalla ricerca di informazioni online, alterando il dibattito pubblico che diventa meno informato[16].

Andrebbero doverosamente analizzate le amplificazioni del tracciamento se messo in atto da imprese in posizione dominante, all'interno di mercati caratterizzati da elevati livelli di concentrazione.

L'opacità dell'ecosistema ad-tech, inoltre, si riflette anche sui profili di responsabilità dei diversi operatori, in particolare delle parti terze. Nella misura in cui queste contribuiscono a definire gli scopi del trattamento, le parti terze devono assicurarsi che il trattamento riposi su una base giuridica valida, anche se non sono direttamente coinvolti nel trattamento dei dati personali[17].

---

[12] Il Google Play Advertising ID, assegnato ad ogni dispositivo Android, è inviato a 70 diverse parti terze. Gli ulteriori operatori sono i *publisher* e i *marketer*. Lo stesso studio ha evidenziato che anche se l'utente fa opt-out (opzione già di per sé non in linea con il principio di protezione dei dati per impostazione predefinita) per finalità di profilazione commerciale, le applicazioni utilizzano l'ID per altri scopi, conferendo una mera illusione di scelta per l'utente; s*upra* n. 10.

[13] Australian Competition and Consumers Commission contro Google Australia PTY LTD & ANOR, notice of filing, ottobre 2019; Data Protection Commission (Irlanda), Data Protection Commission launches Statutory Inquiry into Google's processing of location data and transparency surrounding that processing, comunicato stampa, febbraio 2020.

[14] A. EZRACHI, M. STUCKE, *The Rise of Behavioural Discrimination,* Oxford and University of Tennessee Legal Studies Research Paper n. 54, 2016, p. 2.

[15] C. Cadwalladr, E. Graham-Harrison, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, the Guardian, marzo 2018.

[16] National Telecommunications and Information Administration of the United States Department of Commerce, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities, maggio 2016.

[17] Commission Nationale de l'Informatique et des Libertés (Francia), decisione n. 42 del 30 ottobre 2018 contro Vectuary. L'autorità di protezione dei dati francese ha rilevato che la società ad-tech francese non utilizzava una valida base giuridica per il trattamento, in quanto il consenso richiesto tramite l'Interactive Advertising Bureau (IAB) era considerato insufficiente.

2.2. Pratiche abusive di sfruttamento

L'ecosistema digitale è pervaso dall'utilizzo di interfacce manipolative[18] che spingono l'utente a scelte che non massimizzano la sua utilità[19].

Un esempio empirico è dato dal meccanismo che rende possibile la trasmissione dei dati degli utenti di un social network ai siti web/app di terzi e viceversa, per l'uso dei dati per finalità di profilazione e commerciali. Tale pratica è stata definita aggressiva in quanto idonea a limitare considerevolmente la libertà di scelta o di comportamento del consumatore, mediante indebito condizionamento[20]. Quella di integrare le funzionalità della piattaforma social media con quelle di siti web/app di terzi e di trasferire, conseguentemente, i propri dati a terzi e viceversa è una decisione che l'utente medio, in altre parole, non prenderebbe[21].

Pratiche come quelle descritte hanno un impatto rilevante sui diritti fondamentali. È stato dimostrato che l'individuo è portato a compiere scelte che non risultano efficaci per la protezione dei suoi dati e della sua sfera di riservatezza ed intimità[22].

Questa analisi è rilevante sotto almeno due profili, il primo con significato per il diritto della concorrenza, il secondo con significato per la disciplina di protezione dei dati personali.

In primo luogo, l'individuo risulta gravemente compromesso nella sua autonomia decisionale. L'utente è invalidato nell'apprezzamento delle caratteristiche e della qualità del prodotto, compreso il livello di protezione dei diritti offerto, e finanche nella capacità di comparazione tra prodotti e servizi.

In secondo luogo, in un ecosistema siffatto, sussistono forti dubbi che il consenso dell'individuo possa costituire una valida base giuridica del trattamento, essendo esso di fatto privato dei requisiti di legge[23]. Questa constatazione è drammaticamente

---

[18] Forbrukerradet, Deceived by design, How tech companies use dark patterns to discourage us from exercising our rights to privacy, giugno 2018.

[19] A. ACQUISTI, C. TAYLOR, L. WAGMAN, *The Economics of Privacy*, in *Journal of Economic Literature*, 2016; Sloan Foundation Economics Research Paper n. 2580411, marzo 2016, p. 7, per i quali, assunta una situazione di monopolio, l'adozione di tecnologie tracking conduce ad una condizione sub-paretiana per i consumatori che valutano la qualità del prodotto.

[20] Autorità garante del mercato e della concorrenza, Provvedimento n. 2743, Facebook – condivisione dati con terzi, novembre 2018.

[21] *Ibid.*

[22] *Supra* n. 19. Queste argomentazioni aggravano lo scenario, già critico, di mancata consapevolezza dell'utente, evidenziato dalla dottrina della cd. asimmetria informativa. Si veda, per tutti: G. A. AKERLOF, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, in *The Quarterly Journal of Economics*, p. 488 ss., agosto 1970.

[23] Il consenso deve essere espresso mediante un atto positive con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali, considerando n. 32 GDPR. G. Buttarelli, Big tech is still violating your privacy, the Washington Post, agosto 2018: «asking for an individual's consent should be regarded as an unusual request, given that asking for consent often signals that a party wants to do something with personal data that the individual may not be comfortable with or might not reasonably expect».

problematica se vi si aggiunge, com'è d'uopo, che nel caso di profilazione e tracciamento il consenso è stata descritto come la sola base giuridica ammessa[24]. L'assenza di una valida base giuridica per la profilazione a finalità commerciale è stata riscontrata anche nei confronti della maggiore impresa adtech, non avendo questa messo l'utente in condizione di esprimere un consenso in forma specifica ed inequivocabile[25].

2.3. Concentrazione dei mercati digitali e strategie conglomerali

In un ampio numero di settori, i mercati sono interessati da livelli elevati di concentrazione e dall'operare di un numero incredibilmente ridotto di multinazionali[26]. Il fenomeno interessa in particolare i mercati digitali, nei quali sono attive le più grandi imprese per capitalizzazione economica[27] e dove la concentrazione è persistente[28]. La concentrazione di potere di mercato non era, tra l'altro, attesa agli albori dell'Internet[29]. I mercati digitali dunque amplificano la naturale tendenza verso la concentrazione del capitalismo moderno; oggi una manciata di imprese esercita globalmente più potere e influenza di quanto ogni altra entità privata abbia potuto fare nell'ultimo secolo[30.] La persistente ingerenza nella sfera privata degli individui risulta drammatizzata in mercati tendenti al monopolio[31].

[24] Gruppo di lavoro art. 29, Parere 6/2014 sulla nozione di interesse legittimo del titolare del trattamento. Il tracking e la profilazione per scopi di marketing diretto, pubblicità comportamentale, pubblicità basata sulla geolocalizzazione o servizi di ricerca basati sul tracking, richiedono il consenso espresso (opt-in). L'obbligazione contrattuale e l'interesse legittimo non possono formare valida base giuridica per il trattamento, perché, nel caso del contratto, non può asserirsi che la profilazione per fini di pubblicità commerciale rappresenti una condizione necessaria per lo svolgimento del contratto. Quanto all'interesse legittimo, affinché esso valga come base giuridica, questo deve essere valido, sufficientemente articolato e rappresentare un interesse reale. Inoltre, di per sé richiede di operare un bilanciamento tra l'interesse e i diritti fondamentali dell'interessato che tenga conto delle ragionevoli aspettative di quest'ultimo, ad esempio, a che non sia realizzato un trattamento ulteriore. A fronte di tale aspettativa, il gruppo di lavoro si è espresso nel senso che l'interesse alla monetizzazione non può dirsi sufficiente.
[25] Commission nationale de l'informatique et des libertés (Francia), delibera SAN-2019-001 del 21 gennaio 2019 che emette una sanzione contro Google LLC.
[26] Fondo Monetario Internazionale, Working Paper WP/18/137, Global market power and its macroeconomics implications, giugno 2018, p. 16 ss.
[27] J. Crémer, Y. A. de Montjoye, H. Schweitzer, Competition policy for the digital era, Rapporto finale per la Commissione europea, marzo 2019, p. 13.
[28] Digital competition expert panel, Unlocking digital competition, rapporto finale per il governo UK, marzo 2019, p. 38 ss.
[29] *Supra n. 27*
[30] George J. Stigler Centre for the study of the economy and the state, Committee for the study of digital platforms market structure and antitrust subcommittee, Final Report, maggio 2019, p. 142.
[31] *Ibid*.

Si è evidenziato che l'accresciuta concentrazione dei mercati può avere anche conseguenze politiche: maggiore la concentrazione economica dei mercati, più concentrato (e meno pluralista) è il potere politico[32].

Degna di menzione è anche l'analisi della relazione tra concentrazione del mercato ed innovazione. È stato evidenziato che maggiore è il potere di mercato, minori sono gli incentivi ad innovare[33]. In particolare, ciò è evidente per le imprese che si trovano più prossime alla barriera tecnologica[34]. La mancanza di incentivi all'innovazione, fondata sul rispetto dei diritti e che metta al centro l'individuo, solleva preoccupazioni anche sotto il profilo di protezione dei dati personali, oltre che per quello delle politiche di regolazione dei mercati. All'opposto, mercati competitivi favoriscono l'innalzamento degli standard nella tutela dei diritti, compreso quello alla vita privata e alla protezione dei dati[35].

La maggiore concentrazione dei mercati digitali è il risultato di alcune caratteristiche precise: ad esempio, degli effetti di rete e delle economie di scala e di scopo. Tuttavia, elementi esogeni hanno alimentato i livelli di concentrazione in tali mercati. Nell'ultima decade, le imprese già leader nei mercati di riferimento hanno perseguito una strategia aggressiva di acquisizioni e fusioni rivolte ad altre imprese attive in mercati limitrofi[36]. Un cospicuo numero di acquisizioni è stato realizzato nel settore adtech, ove le imprese target hanno rappresentano uno strumento agile per monetizzare i dati ed accedere al mercato di riferimento[37].

Un numero importante delle fusioni che si registrano nei mercati digitali è conglomerale, esse sono volte cioè ad espandere la presenza dell'acquirente su mercati parzialmente o non affatto collegati a quello di riferimento[38]. Soprattutto nelle fusioni conglomerali, l'acquirente potrebbe avere l'incentivo ad effettuare operazioni per rallentare o annullare l'innovazione del potenziale concorrente[39]. È opportuno rilevare

[32] George J. Stigler Centre for the study of the economy and the state, Committee for the study of digital platforms market structure and antitrust subcommittee, Policy Brief, Maggio 2019, p. 9 ss.
[33] *Supra* n. 26. Lo stesso rapporto ha rinvenuto una correlazione positiva tra markup più elevati ed una maggiore concentrazione del mercato.
[34] *Ibid*.
[35] *Supra* n. 30.
[36] Alphabet ha realizzato 228 fusioni, Microsoft 95, Apple 80, Amazon 68. Nel settore dell'intelligenza artificiale, il numero delle concentrazioni è aumentato di sei volte dal 2013 al 2018, si veda: CB Insights: The race for AI: here are the tech giants rushing to snap up Artificial Intelligence Startups, settembre 2019.
[37] R. BINNS, E. BIETTI, *Dissolving Privacy, One Merger at a Time: Competition, Data and Third-Party Tracking*, in *Computer Law & Security Review*, ottobre 2018. Le imprese a cui si fa riferimento sono Alibaba, Amazon, Google e Facebook.
[38] Comunicazione della Commissione europea, Orientamenti relativi alla valutazione delle concentrazioni non orizzontali a norma del regolamento del Consiglio relativo al controllo delle concentrazioni tra imprese (2008/C 265/07), che definisce conglomerali le fusioni tra imprese che non sono in una relazione né orizzontale né verticale.
[39] M. BOURREAU, A. D. STREEL, *Digital conglomerates and EU Competition policy*, Centre for regulation in Europe, marzo 2019.

che almeno tre delle imprese più grandi per capitalizzazione di mercato sono conglomerati ed impegnate in strategie di espansione conglomerale[40].

Le operazioni conglomerali sono problematiche anche in virtù del modello di business discusso precedentemente. La massiccia estrazione dei dati osservati e dedotti, può consentire un'integrazione di funzionalità tali da portare l'impresa a sfruttare il potere di mercato nel mercato primario per espandersi a quello secondario, e cosi via. Inoltre, deve destare preoccupazione la capacità di tali imprese di agire come detentori di un potere quasi regolatorio e[41], di fatto, dettare le condizioni di concorrenza all'interno di un ecosistema[42,] o finanche di accesso ai contenuti, di fatto orientando la produzione, la distribuzione ed il consumo delle informazioni[43]. Nuovamente, l'impatto di una tale tendenza non è esclusivamente economico: il controllo di flussi informativi, in condizioni di mercato come quelle sopra descritte, altera la libera formazione delle opinioni politiche e delle scelte individuali[44] e limita il pluralismo e il libero accesso alle informazioni[45]. Intacca, il nucleo stesso della democrazia e dei sistemi di valori.

3. Riflessioni per una lettura innovativa dei costi

Sussistono preoccupazioni sugli effetti aggregati che la sistemica intrusione nella sfera di intimità e autodeterminazione possa avere sulle nostre società in senso ampio. Nei mercati in cui gli individui non pagano un prezzo monetario, i costi che questi sopportano possono essere indiretti, nascosti, in un mercato collegato e non necessariamente in quello primario, e di lungo periodo[46].

Un'analisi di ampio respiro dovrebbe dunque guardare ai costi e alle esternalità più ampie che possono risultare per la nostra società dal modello di business presentato, dagli abusi di sfruttamento e dagli elevati livelli di concentrazione dei mercati.

3.1. Le esternalità sottovalutate

[40] Questo discorso si applica quantomeno ad Amazon, Alphabet e Facebook. La prima è attiva in e-commerce, pagamenti e credito, cloud computing, produzione cinematografica, distribuzione di programmazione televisiva, editoria, operazioni di spedizione e logistica. La seconda opera in ricerca online e pubblicità, fornitura di software di geolocalizzazione satellitare, sistemi operativi, servizi cloud, elettrodomestici intelligenti, assistenza sanitaria e robotica. La terza ha espanso la propria presenza dai social media alla messaggistica instantanea, realtà virtuale, AI e riconoscimento facciale e mercati di criptovaluta.

[41] O. LYNSKEY, *Regulating Platform Power*, in *LSE Law, Society and Economy Working Papers*, 2017.

[42] Commissione europea, comunicato stampa: La Commissione apre un'investigazione nella possibile condotta anticoncorrenziale di Amazon, luglio 2019.

[43] *Supra* n. 30.

[44] Comitato europeo per la protezione dei dati, Dichiarazione in merito alle ripercussioni delle concentrazioni economiche sulla protezione dei dati, agosto 2018.

[45] Parlamento europeo, Risoluzione del 3 maggio 2018 sul pluralismo e la libertà dei media nell'Unione europea (2017/2209(INI)).

[46] M. S. GAL, D. L. RUBINFELD, *The Hidden Costs of Free Goods: Implications for Antitrust Enforcement,* in *Antitrust Law Journal*, 2018.

In primo luogo, gli individui subiscono un furto della loro capacità di attenzione da parte delle grandi compagnie tech. A fronte di una capacità di attenzione per definizione limitata, gli individui sono invasi da un flusso abnorme di informazioni, anche indesiderate e ne sopportano il relativo costo[47]. Il costo d'attenzione non si sostanza esclusivamente nella incapacità di processare ogni informazione ricevuta, ma anche in quella di direzionare autonomamente la propria attenzione[48].

In secondo luogo, alle big tech sarebbero ascrivibili scelte e condotte commerciali in grado di avere ripercussioni sulla salute, fisica e mentale. L'ecosistema oggetto di analisi sarebbe responsabile di una vera e propria forma di dipendenza digitale[49]. Vi sarebbe un collegamento tra le continue notificazioni push, spesso attive per impostazione predefinita, e disturbi d'ansia, in particolare negli adolescenti[50]. Esisterebbe la possibilità che le big tech determinino una diminuzione nella capacità di percezione dei fenomeni esterni o in quella di richiamare ricordi del passato[51]. L'intero spettro delle relazioni e della coesione sociale è soggetto ad un'alterazione importante[52].

In terzo luogo, la concentrazione persistente che si registra nei mercati digitali sta esacerbando l'ineguale distribuzione di valore nelle nostre società[53]. Tale diseguaglianza opera sia nel rapporto tra imprese leader del mercato e concorrenti (potenziali, soprattutto), sia nel rapporto tra le stesse imprese e consumatori, in entrambi i casi a vantaggio delle prime.

In quarto luogo, si registrano esternalità ambientali[54]. L'analisi esistente punta il dito contro l'inquinamento provocato dei livelli energia e di acqua richiesti per il funzionamento delle banche dati[55].

In quinto luogo, assistiamo ad una appropriazione di spazi privati, ma anche di quelli pubblici, che per definizione devono essere deputati alla formazione e scambio di opinioni, ad esempio politiche, come già analizzato. Gli abusi nel trattamento dei dati personali sono infatti speculari ai fenomeni di manipolazione online e condizionamento

[47] Una proposta per un attentional SSNIP test è presente in T. WU, *Blind Spot: the Attention Economy and the Law*, in *Antitrust Law Journal*, 2017.
[48] *Ibid*. Le *captive audience* sono riferite in dottrina come comunità di utenti incapaci di compiere scelte autonome.
[49] P. Klass, Is Digital Addiction a Real Threat to Kids, the New York Times, giugno 2019.
[50] Associated press, Warning: Reading this on a smartphone may cause anxiety, researchers say, Los Angeles Times, giugno 2019.
[51] G. Carolyn, How Technology is warping your memory, the Huffington post, dicembre 2017.
[52] J. M. Marlowe, A. Bartley, F. Collins, Digital belongings: The intersections of social cohesion, connectivity and digital media, in *Ethnicities*, 2017, p. 85 ss.
[53] M. Kurz, On the Formation of Capital and Wealth: IT, Monopoly Power and Rising Inequality, giugno 2017.
[54] Climate change: Is your Netflix habit bad for the environment? BBC news, ottobre 2018.
[55] N. ENSMENGER, *The Environmental History of Computing*, Baltimora, 2018 p. 7 ss.

delle scelte politiche56. L'impatto sul sistema democratico è analizzato più diffusamente nella sezione seguente.

3.2. Il costo democratico

Una riflessione più ampia, e sofisticata, di come il potere di mercato si esprime impone di considerare aspetti apparentemente non collegati con la struttura del mercato ed il benessere dei consumatori. Tale riflessione impone di gettare luce sul collegamento tra potere economico, e la sua concentrazione[57], e l'espressione di potere politico[58].

La diminuzione della sfera di riservatezza disponibile per l'individuo, frutto della sorveglianza commerciale, si è detto, sortisce l'effetto collaterale di abbassare i livelli fiducia nelle istituzioni governative[59], ed influenza negativamente la propensione degli individui a partecipare alla vita civica, essenziale per assicurare la salute delle democrazie[60].

Potrebbe obiettarsi che la tutela della concorrenza e la protezione dei dati personali non debbano interessarsi al costo per la democrazia che può derivare dalle condotte di mercato analizzate.

In particolare, molta dell'attenzione della dottrina e dei commentatori si è soffermata su un'accezione esclusivamente economista della nozione di benessere dei consumatori, dalla stessa dottrina inteso come obiettivo ultimo delle norme a tutela della concorrenza[61], ed ha concluso che la protezione della struttura democratica non debba formare oggetto dell'attenzione del diritto della concorrenza[62].

---

[56] Information Commissioner's Office, Democracy disrupted, Personal information and political influence, giugno 2018. La storia di due compagnie implicate nello scandalo fake news (Facebook e Cambridge Analytica) è a ben vedere la storia di un intero ecosistema digitale. Il tracciamento per finalità politiche è, del resto realizzato, dal punto di vista delle tecnologie utilizzate, con gli stessi strumenti del tracciamento per finalità commerciali (*plug-in*, *beacon*, ecc.).

[57] *Supra* n. 30.

[58] R. H. LANDE, S. VAHEESAN, *Preventing the Curse of Bigness Through Conglomerate Merger Legislation*, in *Arizona State Law Journal*, 2019. Gli autori sostengono una presunzione di incompatibilità delle fusioni che coinvolgono imprese con un patrimonio superiore ai 10 bilioni. Per individuare le espressioni potere politico, è utile guardare alla capacità di influenza sul legislatore, attraverso la formulazione di argomentazioni tecnico/legali che smantellino la necessità od efficienza di politiche o regolamentazioni. Oppure, considerare il finanziamento della ricerca, ad esempio attraverso donazioni alle università e la conseguente influenza sulle tematiche che poi ispirano la legislazione. Si veda su questo punto: Garante europeo della protezione dei dati, Parere preliminare su dati personali e ricerca scientifica, gennaio 2020.

[59] Ipsos Mori, Global survey reveals widespread distrust on personal data usage by companies and governments, gennaio 2019, disponibile al https://www.ipsos.com/ipsos-mori/en-uk/global-survey-reveals-widespread-distrust-personal-data-usage-companies-and-governments.

[60] Garante europeo della protezione dei dati, Parere su manipolazione online e dati personali, marzo 2018.

[61] R. A. POSNER, *Antitrust Law*, Chicago, 2001.

[62] C. SHAPIRO, *Antitrust in a time of populism*, in *International Journal of Industrial Organization*, 2018, p. 714 ss.

Un'altra parte della dottrina, che qui si intende con più attenzione analizzare, ha invece posto il nesso concorrenza - democrazia al centro della propria analisi. Essa ritiene che il diritto della concorrenza sia finalizzato a prevenire ogni distorsione al più ampio processo competitivo che crei un pregiudizio all'interesse pubblico[63]. Non è, dunque, il benessere dei consumatori in chiave economista l'obiettivo finale della tutela della concorrenza, ma la creazione di un ordine economico propriamente umano, libero e democratico, ottenibile bilanciando l'efficienza dei processi e dinamiche di mercato con altri scopi di natura deontologica[64]. Tanto quanto la democrazia, la tutela della concorrenza deve tendere alla dispersione del potere, condizione necessaria per preservare la rivalità del mercato[65], secondo una logica di check and balance che consenta a ciascun operatore di limitare il potere del concorrente[66]. La concentrazione del potere di mercato altera questi meccanismi e attribuisce il privilegio di esercitare la limitazione del potere altrui solo ai già leader del mercato, i quali di fatto contribuiscono a determinare le regole del gioco della concorrenza. La concentrazione riduce anche il numero di alternative disponibili sul mercato e limita la libertà di scelta del consumatore[67].

La capacità del potere economico di esprimersi nella vita politica e pubblica era ben nota almeno ad uno dei fautori dell'idea di privacy intesa come libertà dal condizionamento altrui e dell'idea di antitrust intesa come sistema di norme contro l'eccesso di potere[68].

È invece consolidata, anche nella giurisprudenza comunitaria, l'opinione secondo cui privacy e protezione dei dati sono fondamentali allo stato di democrazia[69].

In primo luogo, la compromissione dei diritti alla riservatezza e alla protezione dei dati è in grado di minare l'essenza stessa di una società democratica. La Corte di giustizia ha, ad esempio, evidenziato che la conservazione dei dati e il loro ulteriore utilizzo, in mancanza di informazione agli interessati, può ingenerare la sensazione che la propria vita privata sia oggetto di costante sorveglianza[70].

---

[63] E. DEUTSCHER, S. MAKRIS, *Exploring the Ordoliberal Paradigm: The Competition-Democracy Nexus*, in *Competition Law Review*, 2016 p. 181 ss.

[64] P. BEHERENS, *The Ordoliberal Concept of 'Abuse' of a Dominant Position and its Impact on Article 102 TFEU* in F. DI PORTO (a cura di), *Abusive Practices in Competition Law*, Cheltenham, 2018.

[65] *Ibid.*

[66] In materia di contestabilità dei mercati, si veda anche M. Bourreau, A. d. Streel, *supra* n. 39.

[67] *Supra* n. 64, p.11.

[68] L. D. BRANDEIS, *A curse of Bigness*, in *Harper's Weekly*, New York, 1914.

[69] Ogni interferenza con tali diritti deve essere proporzionata allo scopo perseguito e necessarie in una società democratica, art. 52 della Carta europea dei diritti fondamentali, come interpretata dalla Corte di giustizia.

[70] Sentenza della Corte di giustizia (Grande Sezione) dell'8 aprile 2014, *Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform e altri*, C-293/12 e C-594/12, ECLI:EU:C:2014:238, paragrafo 37.

In secondo luogo, i diritti alla riservatezza e alla protezione dei dati personali sono strumentali al godimento degli altri diritti e libertà fondamentali che informano le nostre democrazie, ad esempio alla libertà di espressione[71].

Tanto la tutela della concorrenza, quanto il diritto alla riservatezza e quello alla protezione dei dati creano quindi e preservano le condizioni che rendono possibile l'esercizio dei diritti e delle libertà[72]. Dal presupposto dell'intrinseca interazione tra le due branche del diritto muovo i paragrafi successivi, tesi ad indicare strumenti operativi per il dialogo tra le discipline.

4. Elementi per l'elaborazione di nuove teorie del danno concorrenziale

Il rapporto tra diritto in materia di protezione dei dati personali, tutela della riservatezza e diritto della concorrenza può essere analizzato secondo almeno due diversi approcci.

Il primo approccio consiste nell'integrare considerazioni di tutela della privacy e dei dati personali all'interno del diritto della concorrenza. Questo perché alcune pratiche, indubbiamente rilevanti per la disciplina in materia di protezione dei dati personali, hanno a ben vedere un significato autonomo e specifico nell'ambito del diritto della concorrenza. Questa metodologia è perseguibile ad ordinamento giuridico (quasi) invariato, attraverso l'adattamento o la formulazione di nuove teorie del danno concorrenziale che muovano dalla comprensione della valenza del dato personale nei rapporti con i concorrenti e i consumatori. Riposa inoltre sull'idea di fondo che i due ordinamenti giuridici, benché incidentalmente connessi, debbano restare autonomi. Nel fornire - in questa sezione - elementi per l'elaborazione di nuove teorie del danno concorrenziale, che facciano leva sul (mancato rispetto degli) obblighi di correttezza e necessità del trattamento e di limitazione della finalità del trattamento, il presente contributo intende contribuire al primo approccio.

Il secondo approccio tende ad una convergenza più marcata tra le due discipline. Muove dall'idea per cui sia il diritto della concorrenza sia il diritto in materia di protezione dei dati personali sono attraversati dalle stesse due tensioni finali: riequilibrare i rapporti di potere (accezione negativa)[73], creare le condizioni per il godimento e

[71] Sentenza della Corte di giustizia (Grande Sezione) del 21 dicembre 2016, *Tele2 Sverige AB contro Post-och telestyrelsen e Secretary of State for the Home Department contro Tom Watson e altri*, C-203/15 e C-698/15, ECLI:EU:C:2016:970, paragrafi 37 e 101, dove per la Corte: «la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione potrebbe […] avere un'incidenza sull'utilizzazione dei mezzi di comunicazione elettronica e, dunque, sull'esercizio, da parte degli utenti, […] della loro libertà di espressione».

[72] G. BUTTARELLI, *This is not an article on data protection and competition*, in *CPI Chronicle*, febbraio 2019.

[73] Almeno per i casi in cui il consenso, l'interesse legittimo e il contratto formino la base giuridica del trattamento. Nella proposta di riforma della normativa di protezione dei dati presentata dalla Commissione si vietava il ricorso al consenso nei casi di *significant power imbalance*, in una previsione poi stralciata dal Parlamento europeo. C. CUIJPERS, N. PURTOVA, E. KOSTA, *Data Protection Reform and the Internet: The Draft Data Protection Regulation*, in A. SAVIN, J.

l'esercizio dei diritti (accezione positiva)[74]. Tale approccio potrebbe condurre ad un'applicazione dei due ambiti propriamente coordinata, finanche gestita da un'autorità unica. Nell'indicare linee di intervento per un'applicazione convergente delle due discipline - nella sezione successiva - lo scritto contribuisce a delineare anche questo secondo approccio, senza pretesa di esaustività e rimandando ad approfondimenti futuri la disamina di ulteriori strumenti operativi per un'applicazione convergente delle due discipline.

4.1. Trattamento eccessivo dei dati

Una parte della dottrina ha sostenuto che la mastodontica accumulazione di dati e la sistematica interferenza con la privacy degli individui che l'economia digitale realizza è eccessiva[75]. Questa osservazione si basa su valutazioni di diritto alla protezione dei dati ed ha conseguenze dirette, come si vedrà, per il diritto della concorrenza. Il caso del tracciamento realizzato da parti terze, precedentemente analizzato, è illustrativo di un trattamento eccessivo[76].

Occorre innanzitutto definire il concetto di "eccessività", ai sensi della normativa in materia di protezione dei dati.

4.1.1. Correttezza (ed equità) del trattamento

Soccorre in questo senso anzitutto la nozione di correttezza, fondamentale alla protezione dei dati[77] e comune anche al diritto della concorrenza e diritto dei consumatori[78]. Nel GDPR, l'obbligo a che il trattamento sia corretto è posto sullo stesso piano della sua liceità[79]. L'obbligo di porre in essere un trattamento corretto impone ad esempio che l'interessato sia informato dell'esistenza di una profilazione e delle conseguenze della stessa[80].

TRZASKOWSKI (a cura di), *Research Handbook on EU Internet Law*, Cheltenham, 2014. Non va taciuto il ruolo chiave che anche la normativa di protezione dei consumatori svolge in questo senso. N. HELBERGER, F. Z. BORGESIUS, A. REYNA, *The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law*, in *Common Market Law Review*, 2017.

[74] Come anticipato, Louis Brandeis mise in luce il ruolo dell'antitrust nel preservare l'idea di democrazia e impedire ad attori privati di diventare talmente potenti da offuscare la stessa idea di Stato di diritto. Si veda: S. D. Warren; L. D. Brandeis in G. Buttarelli, *supra* n.72.

[75] V. H. S. E. ROBERTSON, *Excessive data collection: Privacy considerations and abuse of dominance in the era of big data*, in *Common Market Law Review*, 2020, p. 161 ss.

[76] A. EZRACHI, V. H. S. E. ROBERTSON, *Competition, Market Power and Third-Party Tracking,* in *World Competition: Law and Economics Review*, 2019, p. 5 ss.

[77] D. CLIFFORD, J. AUSLOOS, *Data Protection and the Role of Fairness*, CiTiP Working Paper n. 29, 2017.

[78] I. GRAEF, D. CLIFFORD, P. VALCKE, *Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law*, in *International Data Privacy Law*, 2018, p. 200 ss.

[79] Art 5(1) lett. a), GDPR.

[80] Considerando n. 60, GDPR.

L'indebita accumulazione di dati realizzati attraverso il tracciamento di terze parti e l'invasione onnipresente nella sfera privata dei singoli non può rappresentare una condizione equa per la definizione del rapporto con l'interessato[81].

4.1.2. Necessità del trattamento

In secondo luogo, soccorre a definire l'"eccessività" anche la nozione di necessità del trattamento.

Nel GDPR, almeno due previsioni contengono un riferimento diretto a questa nozione[82]:

il principio di minimizzazione dei dati prescrive che i dati personali debbano essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati[83].

Il principio di protezione dei dati per impostazione predefinita prescrive che il titolare del trattamento metta in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento[84].

Può affermarsi che un trattamento non necessario un è trattamento eccessivo, in particolar modo se non necessario per la prestazione del servizio o la fornitura del bene.

Le previsioni di cui sopra offrono un importante benchmark di riferimento per affermare che, ad esempio, un trattamento che non rispetti il principio di minimizzazione dei dati, o che non rispetti il principio di protezione dei dati per impostazione predefinita, sia un trattamento eccessivo[85].

Nell'ottica in cui i dati personali costituiscano la controprestazione non monetaria pagata dall'utente a fronte della fornitura di un servizio digitale, un trattamento eccessivo dei dati da parte di imprese in posizione dominante può rappresentare un'ipotesi di prezzo

[81] *Fairness* è in italiano correttezza, ma anche equità.

[82] Per completezza d'analisi, vi sarebbe anche la previsione che, nel caso in cui il contratto sia la base giuridica, prescrive che il trattamento sia lecito quando «[...] è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso» (art. 6(1) lett. b) GDPR). Tuttavia, è stato chiarito che le attività di tracking online non possono trovare nel contratto la valida base giuridica per il trattamento. *Supra* n. 24 e da ultimo: Comitato europeo della protezione dei dati, Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, ottobre 2019.

[83] Art. 6(1) lett. b), GDPR.

[84] Art. 25, GDPR; Comitato europeo per la protezione dei dati, Linee guida 4/2019 sul principio di protezione dei per impostazione predefinita, versione per consultazione pubblica, novembre 2019.

[85] Al tempo stesso, nell'interpretazione del regolamento generale, manca un'indicazione univoca sulle circostanze che rendano il trattamento necessario rispetto ad una specifica finalità, nei casi rilevanti per il tracciamento online. Le autorità di protezione dei dati svolgono un ruolo cruciale nel determinare quando l'eccessiva accumulazione dei dati raggiunga una soglia di non necessità del trattamento.

eccessivo o di altra condizione transattiva non equa, vietata dall'articolo 102 del Trattato sul funzionamento dell'Unione europea (TFUE)[86].

Ricorrere alla fattispecie di prezzo eccessivo rischierebbe tuttavia di tradire il carattere di diritto fondamentale dei diritti alla privacy e protezione dei dati personali[87]. Sarebbe dunque ancora più appropriato, nelle circostanze delineate, profilare una fattispecie di abuso di sfruttamento per condizioni di transazione inique. In conclusione, l'articolo 102 TFUE è depositario di una potenzialità inespressa, la cui attivazione, possibile nel pieno rispetto dei trattati, è in grado, se supportata dall'interpretazione fornita dalla protezione dei dati, di sanare le condizioni di squilibrio di transazione che si registrano nei mercati digitali.

4.2. Aggregazione di trattamenti, consenso e finalità

L'economia digitale realizza, come precedentemente visto, un'integrazione tra le funzionalità dei servizi offerti, spesso presentati come unico pacchetto (c.d. bundling).

Indagata soprattutto come condotta rilevante per il diritto della concorrenza[88], il bundling solleva importanti interrogativi per la protezione dei dati.

In primo luogo, la presentazione dei servizi in pacchetto unico comporta una parallela aggregazione del consenso dell'utente, che con un'unica azione presta la propria volontà rispetto a molteplici trattamenti. Nei casi in cui il consenso costituisca la base giuridica del trattamento, deve dubitarsi della liceità dello stesso[89], soprattutto rispetto al requisito della granularità.

Ancora più significativamente, il bundling accorpa un numero abnorme di trattamenti, ciascuno con una diversa finalità, sotto lo stesso capello[90]. I dati personali, in base al principio di finalità del trattamento, devono essere raccolti per finalità

[86] F. COSTA-CABRAL, O. LYNSKEY, *Family ties: the intersection between data protection and competition in EU Law*, in *Common Market Law Review*, 2017, p. 11 ss.; Garante europeo della protezione dei dati, Parere su un'applicazione efficace delle normative nell'economia della società digitale, settembre 2016.

[87] Garante europeo della protezione dei dati, Parere sul pacchetto legislativo un "New deal per i consumatori", ottobre 2018. A. EZRACHI, D. GILO, *The Darker Side of the Moon: Assessment of Excessive Pricing and Proposal for a Post-Entry Price-Cut Benchmark*, in A. EZRACHI (a cura di), *Article 82 EC: Reflections on its Recent Evolution,* Oxford, 2009, hanno anche lamentato l'ulteriore difficoltà oggettiva di stabilire quale sia il livello di controprestazione eccessiva nei mercati in cui non c'è pagamento di prezzo monetario.

[88] Per un esempio di *bundling* censurato si veda: European Commission, Caso AT.40099, Google Android, luglio 2018, che ha *inter alia* dichiarato illecito il bundle Google Play Store/ Google Search app/Google Chrome browser presente sui dispositivi Android.

[89] Gruppo di lavoro art. 29, Linee guida sul consenso nel contesto del regolamento 2016/679, aprile 2018.

[90] Johnny Ryan, O. Lynskey, Response to consultation regarding "online platforms and digital advertising", febbraio 2020, dove si evidenzia che Google avrebbe più di settecento finalità di trattamento condensate in un unico alveo.

determinate, esplicite e legittime, e successivamente trattati in un modo che non sia incompatibile con tali finalità[91].

Valido consenso e finalità del trattamento sono anche indissolubilmente legati. L'interessato deve essere in grado di poter prevedere lo scopo per il quale i suoi dati verranno trattati e non essere colto di sorpresa rispetto allo stesso[92]. Inoltre, se il consenso è aggregato come aspetto non negoziabile di termini e condizioni, esso si presume essere non libero[93].

Il bundling dei trattamenti, del consenso e delle finalità rileva anche ai fini dell'articolo 102 TFUE, a norma del quale la subordinazione della conclusione di contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari, per loro natura non presentanti un nesso con l'oggetto dei contratti stessi, è incompatibile con il mercato interno.

Una rigorosa applicazione del principio di limitazione della finalità potrebbe essere di per sé sufficiente ad assicurare che il potere di scelta genuina del consumatore, che le decisioni in materia di bundling intendono tutelare[94], non risulti compromessa.

5. Linee di intervento per un'applicazione rinforzata e concertata del diritto della concorrenza e della protezione dei dati

Il contributo muove dal presupposto fondamentale che non tutte le questioni relative alla natura riservata dei dati a carattere personale rientrano, in quanto tali e di per sé, nel diritto della concorrenza[95]. Tuttavia, il controllo dei dati personali e l'ingerenza nella sfera di riservatezza degli individui acquistano un significato specifico per il diritto della concorrenza (soprattutto) nei casi di particolare od eccezionale dominanza. La principale argomentazione sostenuta è che sulle imprese che versano in posizione di dominanza nei mercati digitali incombe un obbligo specifico, sotto il duplice profilo del diritto della concorrenza e della protezione dei dati, di assicurare che le rispettive normative non siano tradite. Nel diritto alla concorrenza, si farà riferimento alla nozione di responsabilità speciale. Nella protezione dei dati, all'approccio basato sul rischio e alle obbligazioni scalabili.

Tale disamina è tesa a sostenere che un'applicazione concertata delle due discipline, che faccia leva in particolare sulla nozione di responsabilità speciale e su quella dell'approccio basato sul rischio, consentirebbe di ristabilire gli importanti squilibri contrattuali e di relazioni di potere che attraversano i mercati digitali.

[91] Art. 5(1) lett. b), GDPR.
[92] Gruppo di lavoro art. 29, Linee guida sulla trasparenza nel contesto del regolamento 2016/679, maggio 2018.
[93] *Supra* n. 89, p. 5.
[94] *Supra* n. 88.
[95] Sentenza della Corte di giustizia del 23 novembre 2006, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito contro Asociación de Usuarios de Servicios Bancarios,* C-238/05, ECLI:EU:C:2006:734, paragrafo 63.

5.1. La nozione di responsabilità speciale nel diritto della concorrenza

Il diritto dell'Unione europea non osta a che un'impresa sia in posizione dominante e possa competere sulla base dei propri meriti. Secondo la giurisprudenza della Corte di giustizia, la posizione di dominanza deve essere intesa come quella situazione di potenza economica grazie alla quale l'impresa che la detiene è in grado di impedire una concorrenza effettiva sul mercato di cui trattasi ed ha la possibilità di tenere comportamenti indipendenti rispetto ai suoi concorrenti, clienti e, in ultima analisi, consumatori[96].

Tuttavia, sull'impresa che non avverte la pressione competitiva dei mercati, e che può agire in senso indipendente dalle forze di mercato, incombe una responsabilità speciale. Quella di impedire che il suo comportamento ostacoli una concorrenza realmente priva di distorsioni nel mercato comune[97], dunque che le sue condotte possano distorcere il buon funzionamento e il gioco della concorrenza.

La nozione di responsabilità speciale trova un accoglimento implicito nei trattati. La stessa categoria dell'abuso ex. art. 102 TFUE risulta essere di per sé speciale, in quanto censura una condotta che, assente la posizione dominante, non assurgerebbe a violazione delle norme del diritto della concorrenza[98].

La nozione di responsabilità speciale è presente nella giurisprudenza della Corte di giustizia a far data dal 1983. In quell'anno la Corte affermava che la contestazione della posizione dominante significa che l'impresa in questione, indipendentemente dalle cause di tale posizione, è tenuta in modo particolare a non compromettere col suo comportamento lo svolgimento di una concorrenza effettiva e non falsata nel mercato comune[99].

Poiché il concetto che si discute, come definito in particolare dalla giurisprudenza, sembra essere particolarmente ampio, una parte della dottrina lo mette in collegamento non solo con l'esigenza di preservare la struttura competitiva dei mercati ed evitare

[96] Sentenza della Corte di giustizia del 13 febbraio 1979, *Hoffmann-La Roche & Co. AG contro Commissione delle Comunità europee*, C-85/76, ECLI:EU:C:1979:36, paragrafo 38.

[97] Comunicazione della Commissione europea, Orientamenti sulle priorità nell'applicazione dell'articolo 82 del trattato CE al comportamento abusivo delle imprese dominanti volto all'esclusione dei concorrenti, COM (2008) 832.

[98] W. SAUTER, *A Duty of Care to Prevent Online Exploitation of Consumers? Digital Dominance and Special Responsibility in EU Competition Law*, TILEC Discussion Paper n. 2, 2019, p. 4. L'obbligo di non violare l'articolo 102 TFUE impone all'impresa in posizione di dominanza di comportarsi come se fosse soggetta a pressione competitiva, *ibid*. p. 6

[99] Sentenza della Corte di giustizia del 9 novembre 1983, *N.V. Nederlandsche Banden-Industrie-Michelin contro Commissione delle Comunità europee,* C-322/81, ECLI:EU:C:1983:313, paragrafo 57. La nozione è stata poi avallata dalla Corte a più riprese, e più recentemente in: sentenza della Corte di giustizia (Prima Sezione) del 6 dicembre 2012, *AstraZeneca AB e AstraZeneca plc contro Commissione europea,* C-457/10 P, ECLI:EU:C:2012:770, paragrafo 134; sentenza della Corte di giustizia (Seconda Sezione) del 6 ottobre 2015, *Post Danmark A/S contro Konkurrencerådet*, C-23/14, ECLI:EU:C:2015:651, paragrafo 71.

l'esclusione dei concorrenti, ma anche con l'esigenza di evitare comportamenti a danno dei consumatori, come discriminazione e altre forme di abuso di sfruttamento[100].

Discende da tale nozione non solo l'obbligo negativo di evitare la violazione del diritto della concorrenza ma, significativamente, anche l'obbligo positivo di agire secondo i canoni di correttezza definiti dalle norme pertinenti al contesto della discriminazione o dello sfruttamento[101]. È dunque al più ampio complesso normativo, che si applica alla fattispecie, che occorrere guardare. A tal proposito, la Corte di giustizia ha recentemente riconosciuto che il contesto giuridico entro il quale una condotta abusiva si colloca è elemento al quale occorre riferirsi per valutare la valenza anti-competitiva di una pratica[102].

5.1.1. Protezione dai dati come standard normativo per l'identificazione dell'abuso

Le norme a tutela della riservatezza e della protezione dei dati personali formano parte dell'acquis che un'impresa, in posizione di dominanza o meno, deve rispettare. Nei mercati il cui modello di business si fonda sulla sistematica ingerenza nella sfera protetta da tali diritti, tali norme entrano con titolo preferenziale, si potrebbe sostenere, nell'acquis di riferimento, rispetto al quale la più generale correttezza dell'operato delle imprese in posizione di speciale dominanza deve essere valutata.

La violazione della disciplina in materia di protezione dei dati personali è stata utilizzata come parametro per identificare un abuso di posizione dominante, ed affermare che le imprese in posizione dominante sono soggette ad obblighi speciali per il diritto della concorrenza[103]. Il fatto che un'impresa dominante nel mercato dei social media, come quella oggetto del caso, abbia violato la normativa posta a presidio della tutela dei dati personali rappresenterebbe ipso facto uno sfruttamento abusivo nei confronti dei consumatori[104]. Nello specifico, la violazione della disciplina in materia di protezione dei dati personali è stata ravvisata nell'aver reso l'utilizzo del servizio dipendente dall'accettazione da parte dell'utente del fatto che l'impresa fosse autorizzata a: 1) raccogliere dati generati dai dispositivi e dagli utenti nei servizi di proprietà dell'impresa e da siti e applicazioni di terze parti; 2) combinare tali dati con quelli dell'account social media. Siffatti termini e pratiche costituiscono abuso di sfruttamento nei confronti dei

[100] *Supra* n. 98.
[101] *Ibid*., p. 11.
[102] Sentenza della Corte di giustizia del 14 marzo 2013, *Allianz Hungária Biztosító Zrt. e altri contro Gazdasági Versenyhivatal,* C-32/11, ECLI:EU:C:2013160, paragrafo 36. In particolare, la Corte si riferisce alla valutazione della restrizione della concorrenza «per oggetto» negli accordi ex. art 101 TFUE. Nell'opinione dei giudici UE, occorre riferirsi al contenuto delle sue disposizioni, agli obiettivi che esso mira a raggiungere, nonché al contesto economico e giuridico nel quale esso si colloca.
[103] Bundeskartellamt prohibits Facebook from combining user data from different sources, comunicato stampa, febbraio 2019.
[104] Bundeskartellamt, sesta divisione, B6-22/16, decisione a norma della sezione 32(1) della legge tedesca sulla concorrenza (GWB).

consumatori. Al contempo, l'impresa in oggetto incorrerebbe anche in una pratica abusiva escludente poiché le condotte descritte consentirebbero un controllo su una mole eccezionale di dati, tali da accordare un vantaggio competitivo importante sugli altri concorrenti, rinforzare le barriere all'ingresso esistenti, e consolidare la posizione di dominanza nei confronti dei consumatori.

La decisione cui si fa riferimento è stata commentata come un passo importante nel percorso in direzione dell'affermazione della disciplina in materia protezione de dati come benchmark normativo per l'identificazione di un abuso[105].

Occorre iniziare riflessioni, sia accademiche che operative, su un aspetto diverso del rapporto tra posizione dominante, responsabilità speciale e normativa in materia di protezione dei dati personali. E cioè chiedersi se la violazione della disciplina di protezione dei dati possa essere strumento a mezzo del quale l'impresa accresce indebitamente la sua presenza nel mercato. Andrebbe dunque esplorata non solo l'idea che la violazione di tale disciplina possa rappresentare un abuso in sé[106], ma anche che la sua sistematica violazione da parte (almeno) dell'impresa in posizione di speciale responsabilità possa condurre alla cristallizzazione di una posizione nel mercato altrimenti non raggiungile da parte della stessa impresa secondo un'idea di concorrenza basata sul merito[107].

[105] G. BUTTARELLI, *Supra* n. 73.

[106] Il giudice della Corte di giustizia Thomas von Danwitz si è espresso nel senso che la sistematica violazione della privacy e protezione dei dati potrebbe essere sanzionata come abuso di posizione dominante ex art. 102 TFUE. Fondamentale sarebbe anche l'assenza di informazioni chiare e trasparenti, disponibili al consumatore, circa la quantità di informazioni personali cedute. Una concezione troppo ristretta del diritto della concorrenza, infatti, rischierebbe di mettere in ombra aspetti relativi alla privacy che invece non vanno oscurati, considerando la vicinanza d'intenti e di scopi delle due discipline. Nelle parole di von Danwitz, l'incertezza circa il prezzo da pagare per la fruizione del servizio o prodotto rappresenterebbe uno dei principali impedimenti ad un sano sviluppo della concorrenza nei mercati basati sullo sfruttamento dei dati. Vedi T. von Danwitz, Privacy and competition law, Statement for the 19th IKK International Conference on Competition, Berlin, marzo 2019, riportato da MLex, "Privacy-abusing tech companies could attract EU antitrust enforcement, judge warns".

[107] D. SRINIVASAN, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, in *Berkeley Business Law Journal*, 2019, p. 39 ss. L'evoluzione delle pratiche di Facebook sui dati personali è qui definita emblematica della relazione tra lo sfruttamento degli utenti e il suo dominio sul mercato. Annunciato come un social media volto a rispondere alle preoccupazioni sulla privacy, una volta che il mercato in oggetto stava diventando meno competitivo, Facebook ha integrato i "Beacon*"* (2007) e i "Mi piace" (2010). Entrambi avrebbero consentito all'azienda di tracciare gli utenti su siti Web e app di terze parti ed entrambi sarebbero stati ingannevolmente pubblicizzati come funzionalità innocenti attraverso le quali gli utenti avrebbero potuto condividere informazioni sui loro interessi sulla piattaforma. Una volta consolidata la posizione dominante dell'azienda, Facebook avrebbe costretto gli utenti ad acconsentire a ciò che prima aveva promesso di mai compiere, vale a dire tracciare gli utenti e rendere l'accettazione del tracciamento condizione necessaria per l'utilizzo del servizio.

Degno di analisi è anche l'aspetto del what comes first nei mercati digitali, se l'abuso di sfruttamento, o la posizione dominante, e il rapporto di causalità[108], e se dunque si può sostenere che l'abuso possa condurre alla dominanza, o quanto meno ad esacerbarla[109].

È dunque ben possibile che un'impresa eccezionalmente dominante possa consolidare la sua posizione dominante attraverso pratiche di sfruttamento e di inganno degli utenti, che violino il diritto fondamentale alla riservatezza e protezione dei dati personali. Simultaneamente, e proprio in ragione della posizione dominante, è ben possibile che la stessa impresa possa procedere a degradare il livello di privacy e protezione dei dati offerto, ben al di sotto del livello competitivo, cioè al di sotto di livello al quale il leader del mercato è astretto in ragione della pressione competitiva[110]. In conclusione, le due dimensioni dell'abuso e della posizione dominante si rinforzano mutualmente.

Da ultimo, va inoltre evidenziata l'interconnessione tra pratiche abusive escludenti e quelle di sfruttamento nei mercati oggetto di analisi. Soltanto una parte ristretta della dottrina ne ha espresso il legame, e l'impatto sulla struttura del mercato[111].

È opinione di chi scrive che gli abusi di sfruttamento possano avere effetti importanti sulla struttura di mercato. In particolare, una raccolta dei dati aggressiva è in grado di: a) degradare il benessere dei consumatori; b) fornire al leader di mercato una conoscenza superiore circa i comportamenti, preferenze e opinioni degli individui, dunque un vantaggio competitivo tale da stigmatizzare la sua posizione nel mercato e renderla non

[108] Sentenza della Corte di giustizia del 13 febbraio 1979, *Hoffmann-La Roche & Co. contro Commissione delle Comunità europee*, C-85/76, ECLI:EU:C:1979:36, paragrafo 27 e sentenza della Corte di giustizia del 21 febbraio 1973, *Europemballage Corporation e Continental Can Company Inc. contro Commissione delle Comunità europee,* C-6/72, ECLI:EU:C:1973:22, paragrafo 27 non richiedono di dimostrare il collegamento causale tra la posizione dominante e l'abuso. Nella sentenza della Corte di giustizia del 14 novembre 1996, *Tetra Pak International SA contro Commissione delle Comunità europee*, C-333/94, ECLI:EU:C:1996:436, paragrafo 27, la Corte presuppone invece il collegamento causale.

[109] Questi profili sono presenti nelle discussioni che hanno seguito la decisione con la quale il tribunale regionale superiore di Düsseldorf ha sospeso in sede di impugnazione il provvedimento emanato dal Bundeskartellamt contro Facebook. Facebook/Bundeskartellamt, decisione del tribunale regionale superior di Düsseldorf (Oberlandesgericht Düsseldorf) in interim proceedings, agosto 2019, Causa VI-Kart 1/19 (V). Secondo l'avviso dei giudici, l'autorità di concorrenza non avrebbe *inter alia* provato il nesso causale tra la posizione di dominanza e l'abuso. Ad avviso dei giudici, l'autorità non avrebbe neppure svolto adeguatamente l'analisi controfattuale, volta a profilare lo scenario che si sarebbe realizzato con condizioni sufficienti di concorrenza. Il tribunale contesta inoltre l'esattezza dell'argomentazione circa l'invalidità del consenso, e sostiene che l'utente è ben in grado di bilanciare, da una parte, l'utilità che deriva dall'utilizzare un social media basato sulla profilazione pubblicitaria e, dall'altra, le conseguenze derivanti da una raccolta ed utilizzo eccessivo dei dati da parte di Facebook.

[110] *Supra* n. 107.

[111] *Supra* n. 64, p. 16, Beherens illustra come la struttura del mercato e le condotte non possano essere isolate l'una dall'altra ma all'opposto siano interdipendenti, senza che il nesso causale debba andare una direzione o nell'altra. Si afferma che le pratiche anticoncorrenziali non devono essere limitate alle pratiche che danneggino i consumatori, ma devono includere pratiche che conducano al consolidamento della posizione di mercato. In altre parole, le condotte abusive di sfruttamento possono avere effetti negative sulla struttura di mercato e viceversa.

contestabile da parte degli altri operatori. S'impone dunque un'analisi generalizzata su come gli abusi di sfruttamento e quelli di esclusione possano autosostenersi a vicenda, e servire gli uni gli scopi degli altri.

5.2. L'approccio basato sul rischio e gli obblighi scalabili nella protezione dei dati

Nel contesto della protezione dei dati, la contropartita della nozione di responsabilità speciale è costituita dall'approccio basato sul rischio. Esso impone ai titolari del trattamento di articolare gli obblighi giuridici che discendono dal regolamento alla luce, appunto, del livello di rischio posto dallo specifico trattamento[112].

Il principio basato sul rischio va ricondotto al più generale principio di responsabilità o responsabilizzazione (cd. accountability) che permea la disciplina di protezione dei dati. Esso richiede che il titolare del trattamento metta in essere misure appropriate ed efficaci di applicazione dei principi e degli obblighi normativi, e di essere pronto a dimostrarne, su richiesta, l'osservanza[113].

L'appropriatezza ed efficacia delle misure deve essere valutata alla luce del rischio coinvolto[114]. Aspetti come le dimensioni delle operazioni di trattamento, gli obiettivi dello stesso e il numero di trasferimenti di dati previsti possono contribuire a definire il livello di rischio[115]. Occorre altresì tenere conto del tipo di dati, in particolare del fatto che si tratti o meno di dati sensibili e della circostanza che l'incaricato del trattamento sia progettista e/o produttore di tecnologie dell'informazione[116]. Se da una parte la forza del GDPR deriva dall'essere ispirato a principi di neutralità tecnologica, dall'altra è vero che una parte della dottrina ha evidenziato come alcune tecnologie, come ad esempio la profilazione o l'analisi inferenziale (invasiva), siano suscettibili di creare nuovi tipi di rischi o di accentuare alcuni rischi esistenti[117].

La disciplina attuale presume che, in alcuni casi, la pratica che coinvolge i dati personali presenti un rischio elevato. Ad esempio, nell'ipotesi in cui il trattamento realizzi una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche. O nell'ipotesi di trattamento, su larga scala, di categorie speciali di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati

[112] Consideranda 75-77, GDPR.
[113] Gruppo di lavoro articolo 29, Parere 3/2010 sul principio di responsabilità, p. 9.
[114] R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation*, in *Computer Law and Security Review*, 2018, p. 279 ss.; K. DEMETZOU, *GDPR and the concept of risk*, in ELENI COSTA ET AL. (a cura di), *Privacy and Identity Management. Fairness, accountability and transparency in the age of big data*, Springer International, Cham, 2019, p. 137 ss.
[115] *Supra* n. 113.
[116] *Ibid.*
[117] S. WACHTER, *The GDPR and the Internet of Things: a three-step transparency model*, in *Journal Law, Innovation and Technology,* 2018.

di cui all'articolo 10[118]. Si tratta di tipologie di trattamento al cuore delle modalità di funzionamento delle big tech, basate sul tracciamento persistente che coinvolge dati sensibili e su trattamenti automatizzati suscettibili di produrre effetti giuridici.

Dall'approccio basato sul rischio discendono obblighi giuridici graduati e proporzionati[119], dunque di diversa ampiezza ed intensità. La diversa articolazione del concetto di rischio non solo determina la portata dell'obbligo giuridico che incombe sul titolare[120], ma anche la circostanza che questi sia o meno soggetto ad un determinato obbligo. Ne sono un esempio gli obblighi di: eleggere un rappresentante del titolare o responsabile del trattamento nell'UE[121], notificare una violazione dei dati all'interessato[122], condurre la valutazione d'impatto sulla protezione dei dati[123], effettuare una consultazione preventiva presso l'autorità di controllo[124], designare il responsabile per la protezione dei dati[125]. La tesi che si intende portare avanti è che tale principio rappresenti il fondamento sul quale formulare l'argomentazione giuridica, anche nello specifico ambito della protezione dei dati, della responsabilità speciale di alcuni operatori di mercato.

Nell'ambito dell'approccio basato sul rischio, la dottrina ha distinto obblighi di mezzo ed obblighi di risultato. Si è sostenuto che sia il principio di minimizzazione dei dati sia il principio limitazione della finalità, rilevanti per definire teorie del danno concorrenziale nuove, letti in combinato disposto danno luogo ad un obbligo di risultato[126]. Il concetto di rischio deve dunque orientare la valutazione circa il fatto, ad esempio, che il trattamento ulteriore sia da considerarsi compatibile con la finalità originaria, per cui meno certo è l'impatto sui diritti e libertà fondamentali, più stringente deve essere la valutazione di compatibilità[127]. Ciò significa che le imprese big tech non dovrebbero solo provare a rispettare tali principi, ma anche riuscirci pienamente.

L'approccio basato sul rischio non sembrerebbe esigere che le autorità nazionali di controllo diano priorità alle pratiche che presentino profili di rischio problematici. Questo a dispetto del fatto che il principio di responsabilità era stato interpretato come

[118] Sono questi casi in cui è obbligatorio condurre una valutazione d'impatto sulla protezione dei dati. Gruppo di lavoro articolo 29, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento «possa presentare un rischio elevato» ai fini del regolamento (UE) 2016/679, aprile 2017, p. 8 ss.
[119] Gruppo di lavoro articolo 29, Dichiarazione sul ruolo dell'approccio basato sul rischio nella protezione dei dati personali, maggio 2014, p. 2.
[120] Un titolare del trattamento il cui trattamento di dati non presenti elevato rischio non dovrà fare tanto quanto un titolare il cui trattamento presenti rischio elevato per rispettare la legislazione, *ibid*.
[121] Art. 27, considerando 80, GDPR.
[122] Art. 33, consideranda 85, 87 e 88, GDPR.
[123] Art. 35, consideranda 84, 89-93 e 95, GDPR.
[124] Art. 36, consideranda 94-96, GDPR.
[125] Art. 37, considerando 97, GDPR.
[126] C. QUELLE, *The risk-revolution in Eu data protection law: we can't have our cake and eat it, too*, in *Tilburg Law School Legal Studies Research Paper Series*, 2017.
[127] *Ibid.*

«utile alle autorità di protezione dei dati, […per aiutarle ad] essere più selettive e strategiche»[128]. Dovrebbe invece sostenersi che, alla luce dei parametri sopra esposti (estensione, numero trasferimenti, tipo di dati), maggiore è il rischio atteso dal trattamento, maggiore dovrebbe essere l'attenzione delle autorità di controllo.

Una dottrina ha proposto che gli strumenti di diritto della concorrenza, ad esempio la definizione del mercato rilevante e del potere di mercato, possano contribuire ad interpretare la portata delle obbligazioni per il titolare e responsabile del trattamento[129]. È fondamentale, tuttavia, rivedere le nozioni, in particolare quella di potere di mercato, alla luce dei fenomeni prima analizzati. Altrimenti, un'importazione de jure condito delle nozioni e degli strumenti come quelli della definizione del potere di mercato consentirebbe di aggiungere poco alla comprensione del funzionamento dei mercati.

Con questi presupposti, la cross-fertilisation tra la nozione di responsabilità speciale e di approccio basato sul rischio è possibile e deve essere perseguita. Questo potrebbe consentire di affermare che l'impresa che versa in posizione di dominanza (nel diritto della concorrenza) è soggetta ad obblighi più stringenti secondo il principio dell'approccio basato sul rischio (nella protezione dei dati), e dovrebbe preoccuparsi con maggiore premura di rendere effettiva l'applicazione del GDPR. Come visto, le pratiche messe in atto dalle big tech vanno al momento in tutt' altra direzione.

In conclusione, il modello di business analizzato comporta operazioni di trattamento dei dati altamente problematiche, che implicano un livello elevato di rischio, per ampiezza, numero dei trasferimenti e tipo di dati personali coinvolti. In considerazione di ciò, le big tech, secondo l'approccio delle obbligazioni graduali, dovrebbero potersi dire gravate da obblighi più stringenti. I grandi titolari del trattamento dovrebbero attuare misure rigorose[130], in linea di principio, ad esempio nel condurre la valutazione d'impatto sulla protezione dei dati o nell'esigenza di trasparenza nel rapporto con gli utenti[131]. Le stesse imprese poi, dovrebbe essere oggetto di uno scrutinio urgente e rinforzato da parte delle autorità competenti.

6. Conclusioni

Il modello di business basato sullo sfruttamento intensivo dei dati personali si è tradotto in un monitoraggio persistente delle vite degli individui. Interfacce manipolative spingono l'individuo a compiere scelte non efficaci sotto il profilo della tutela dei diritti, come ad esempio accettare:

un trattamento eccessivo, non equo, non necessario, dei propri dati personali;

un'aggregazione di trattamenti dei dati e relative finalità.

Entrambe le condotte, come visto, sono censurabili sia nel contesto di protezione dei dati personali, che in quello di diritto della concorrenza.

[128] *Supra* n.113, p.17.
[129] S*upra* n. 78.
[130] *Supra* n.113.
[131] La trasparenza è predicato del principio di responsabilità, *ibid*.

In mercati che sperimentano elevati livelli di concentrazione, come quelli digitali, desta preoccupazione la capacità dei conglomerati di: espandersi dal mercato primario ai mercati secondari fruttando la sorveglianza commerciale di consumatori e concorrenti; dettare le condizioni di concorrenza in un ecosistema o di regolamentare l'accesso ai contenuti ed il flusso di informazioni.

La società sopporta costi aggregati, spesso indiretti e nascosti, in conseguenza della diminuzione della sfera privata di autodeterminazione e della sfera pubblica di partecipazione democratica.

Un'applicazione concertata e rinforzata degli strumenti di protezione dei dati e di diritto della concorrenza consentirebbe di risanare gli importanti squilibri contrattuali e di relazioni di potere che attraversano i mercati digitali.

Sulle imprese che non avvertono la pressione competitiva dei mercati incombe la responsabilità speciale di impedire che la concorrenza sia falsata. Sulle stesse, incombe l'obbligo di agire secondo i canoni di correttezza e liceità definiti dalle norme applicate al contesto di riferimento, in particolare quelle in materia di protezione dei dati personali.

Specularmente, ed in ragione della problematicità sottesa alle operazioni di trattamento, le big tech devono dirsi gravate da obblighi più stringenti di adottare misure rigorose di tutela dei diritti. Dovrebbero essere oggetto, poi, di uno scrutinio urgente e rinforzato da parte delle autorità competenti.

Il diritto della concorrenza mira a garantire che i mercati si assestino su un livello di concorrenza tale da garantire un livello sufficiente di innovazione. Il rispetto della privacy e della protezione dei dati fondamentali, quali connotati essenziali della democrazia[132], deve ispirare un'evoluzione tecnologica sana, virtuosa, sostenibile. È dunque anche nell'interesse dei due diritti fondamentali che i mercati sperimentino dei livelli di sana pressione competitiva, che spingano le imprese a migliorare la qualità di servizi e prodotti offerti. Un elevato livello di concorrenza nei mercati è condizione necessaria affinché si attivi una race to the top nell'adozione di tecnologie che mettano privacy, tutela dei dati e sicurezza al centro del modello di business[133].

[132] S. RODOTÀ, *Intervista su privacy e libertà*, 2005; V. BOEHME-NEßLER, *Privacy: a matter of democracy. Why democracy needs privacy and data protection*, in *International Data Privacy Law*, 2016.

[133] In senso contrario, l'operatore di mercato fronteggia una triste scelta binaria: indugiare nel modello di business prevalente o abbandonare il mercato.

Regolamento europeo n. 679/2016: profili di continuità e aspetti innovativi

DI ALESSANDRA PALLOTTA [*]

SOMMARIO: 1. Premessa. – 2. I diritti degli interessati: diritti "vecchi" e nuovi diritti. – 3. Il principio di *accountability*. – 4. Privacy by default e by design, registro dei trattamenti, valutazione d'impatto, DPO e data breach. – 5. Problematiche aperte. – 6. La dimensione etica della protezione dei dati personali.

1. Premessa

Vorrei innanzitutto esprimere il mio ringraziamento all'organizzazione del Convegno e, in particolare, al professore Francesco Rossi Dal Pozzo, per avermi invitata a parteciparvi. La tematica del Convegno riveste sicura attualità per i molteplici aspetti problematici che sono stati bene evidenziati dalle pregevoli relazioni di questa mattina.

Con la mia relazione intendo approfondire la materia del trattamento dei dati personali a seguito dell'entrata in vigore del Regolamento europeo n. 679/2016 sulla protezione dati; ciò, specie alla luce dell'attività concretamente e quotidianamente svolta dal Garante nell'ambito della tutela dei dati personali, con l'intento di metterne in evidenza i profili di continuità e gli aspetti innovativi rispetto alla disciplina previgente e sottolineandone le maggiori criticità.

La disciplina della materia ha subito, con l'entrata in vigore del Regolamento europeo n. 679, una profonda riconsiderazione, influenzata da una politica europea di armonizzazione tesa a superare le frammentazioni nell'applicazione della disciplina di protezione dati venutasi a creare a seguito dell'attuazione della direttiva 95/46 CE. La globalizzazione e la rapidità dell'evoluzione tecnologica e digitale hanno trasformato i sistemi economici nazionali e sovranazionali, nonché le relazioni sociali e facilitato la libera circolazione dei dati personali all'interno dell'Unione europea determinando una maggiore necessità di regole comuni e coerenti a tutti i Paesi europei, in grado di garantire un elevato livello di protezione dei dati personali.

Con il Regolamento europeo, si è passati da una disciplina fortemente disomogenea e differenziata ad una disciplina uniforme in tutti i paesi dell'Unione europea, caratterizzata da un insieme di regole comuni dei diritti degli interessati e degli obblighi di coloro che effettuano il trattamento dei dati, come pure poteri equivalenti alle Autorità di controllo e sanzioni equivalenti per le violazioni negli Stati membri. Le varie

[*] Funzionario dell'Ufficio del Garante italiano per la protezione dei dati personali

declinazioni nazionali devono ormai trovare un equilibrio nella prospettiva di una comune visione della centralità della persona e dei dati.

In un mondo strutturalmente interconnesso e in una realtà immateriale, quale quella della rete, la barriera territoriale appare sempre più anacronistica.

Una normativa uniforme e comune se, da un lato, è creatrice di omogeneità e armonizzazione, per altro verso, sconta le difficoltà di accomunare, sotto un'unica normativa, realtà e procedure differenti. In tal senso, è chiaramente percepibile che il Regolamento europeo, se rapportato alla vastità del campo applicativo, è formulato in termini concisi e generali, essenzialmente per principi, lasciando qua e là spazi di intervento ai legislatori nazionali.

2. I diritti degli interessati: diritti "vecchi" e nuovi diritti

Se analizziamo i principi espressi dal nuovo Regolamento possiamo notare che sono essenzialmente gli stessi che erano contenuti nell'art. 11 del d.lgs. 196 del 2003 (Codice in materia di protezione dei dati personali); il principio di liceità, finalità, esattezza, minimizzazione dei dati facevano, infatti, già parte della preesistente cultura giuridica. Non sono una novità e si pongono, quindi, in una linea di continuità con la direttiva 95/46.

Se prendiamo in esame i diritti degli interessati (artt. 15 e ss. del Regolamento), possiamo notare che alcuni di questi rappresentano una novità rispetto alla normativa previgente, altri, sebbene già previsti precedentemente, acquisiscono, ora, una rivisitazione.

I diritti degli interessati rappresentano ora, come anche nella previgente disciplina, importanti strumenti di autodeterminazione informativa. Accedendo ai propri dati l'interessato è in grado di controllarne la qualità, potendo richiedere, se del caso, la rettifica e l'integrazione. Attraverso l'opposizione, la richiesta di limitazione o, ricorrendone le circostanze, di cancellazione, l'interessato è in grado di controllare la conformità delle operazioni di trattamento sui propri dati personali al dato normativo. Il denominatore comune è consentire all'interessato di mantenere il controllo sulle informazioni che lo riguardano, informazioni che costituiscono una componente essenziale del diritto all'identità personale.

Il diritto di accesso è il diritto che più di tutti viene esercitato e di cui viene maggiormente chiesta tutela all'Autorità; consente all'interessato di ricevere dal titolare una serie di informazioni a lui riferite, quali, tra le altre, le categorie di dati personali oggetto di trattamento, i destinatari o le categorie di destinatari a cui i dati personali sono o saranno comunicati, il periodo di conservazione dei dati personali, l'origine dei dati personali, l'esistenza del diritto di chiedere al titolare la rettifica o la cancellazione dei dati personali o la limitazione del trattamento, il diritto di proporre reclamo all'Autorità, l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

Tale diritto, con le nuove norme regolamentari, sì è notevolmente ampliato nei contenuti, riferendosi anche al periodo di conservazione dei dati e all'esistenza degli ulteriori diritti riconosciuti all'interessato.

Secondo quanto riferito dalle Linee guida sui diritti degli individui con riguardo al trattamento dei dati personali adottate dall'European Data Protection Supervisor, attraverso il diritto di accesso l'interessato viene a conoscenza di quali sono i suoi dati personali oggetto di trattamento, verifica la qualità dei dati, la liceità del trattamento, esercita consapevolmente gli altri diritti riconosciuti dalla legge. Per questo motivo il diritto di accesso è espressione, più degli altri, del diritto dell'interessato al controllo dei propri dati, in quanto l'interessato è messo nelle condizioni di poter attivare gli ulteriori strumenti posti a sua tutela dalla legge. E ciò spiega anche perché l'esercizio del diritto di accesso sia garantito a prescindere dall'esistenza di una lesione, potenziale od effettiva, lamentata dall'interessato.

Il titolare che riceve una richiesta di accesso non può limitarsi a dare una conferma dell'esistenza dei dati ma deve estrarre i dati dai documenti in suo possesso comunicarli all'interessato in modo completo, in forma intellegibile e, ove richiesto, trasporli su un supporto cartaceo o informatico. Il Regolamento sancisce espressamente l'obbligo del titolare di fornire all'interessato una copia gratuita dei dati personali oggetto di trattamento, il che rappresenta una novità della nuova disciplina in quanto sia la direttiva 95/46 sia il decreto legislativo 196/2003, non prevedevano tale obbligo, salvo che non rappresentasse uno strumento necessario per consentire all'interessato di prendere contezza dei dati personali che lo riguardavano.

Particolare interesse rivestono i diritti nuovi: il diritto all'oblio, il diritto alla limitazione dei dati e il diritto alla portabilità.

Il diritto all'oblio costituisce un diritto alla cancellazione dei dati in forma rafforzata in quanto obbliga il titolare del trattamento che ha reso pubblici i dati, non solo a cancellarli ma anche ad adottare le misure ragionevoli e tecniche per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

E' con la sentenza della Corte di Giustizia dell'Unione Europea del 13 maggio 2014, resa nella causa Google Spain, che viene riconosciuta per la prima volta l'esistenza del diritto all'oblio, quale diritto del singolo alla "deindicizzazione" delle informazioni personali che fossero risultate "non più attuali, irrilevanti o non più rilevanti" rispetto alle finalità del trattamento, ponendo in primo piano il principio di autodeterminazione informativa del soggetto alla conservazione della propria identità digitale. Successivamente, con le Linee guida adottate il 26 novembre 2014, il Gruppo Art. 29 ha definito criteri interpretativi univoci della sentenza Google Spain e individuato un elenco di criteri condivisi ai fini della trattazione dei ricorsi da parte delle Autorità europee per la protezione dei dati.

Il diritto alla limitazione dei dati permette di ottenere dal titolare la limitazione del trattamento quando, tra gli altri casi, l'interessato contesta l'esattezza dei dati, per il periodo necessario al titolare per verificare l'esattezza delle informazioni.

Il diritto alla portabilità dei dati dà diritto all'interessato di ricevere dal titolare i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico e ha il diritto di ottenere la trasmissione di tali dati ad un altro titolare se il

trattamento si basa sul consenso o su un contratto e se il trattamento è effettuato con mezzi automatizzati.

Anche i diritti già disciplinati nella previgente disciplina hanno subito un processo di rivisitazione. La novità che salta subito all'occhio concerne la modalità di attivare la procedura di controllo del Garante. Mentre prima, con il Codice privacy, l'interessato poteva rivolgersi al Garante utilizzando le forme della segnalazione/reclamo e del ricorso, oggi, il Regolamento prevede che l'interessato possa rivolgersi al Garante nella sola forma del reclamo e solo successivamente al periodo di tempo concesso al titolare per rispondere alle richieste dell'interessato.

Questo perché il Regolamento ha previsto che il titolare debba fornire riscontro all'interessato, senza ingiustificato ritardo, e, comunque, al più tardi entro un mese dal ricevimento della richiesta. Il termine previsto può, se necessario, essere prorogato di un mese in ragione della complessità e del numero delle richieste; il titolare deve informare l'interessato entro 1 mese del ricevimento della richiesta di tale proroga e dei motivi del ritardo. Anche nel caso in cui il titolare non sia in grado di ottemperare alle richieste dell'interessato deve darne notizia all'interessato entro un mese specificando le ragioni dell'inottemperanza e della possibilità di proporre reclamo al Garante. Pertanto, se l'interessato proporrà reclamo all'Autorità prima che il periodo temporale di un mese si sia consumato, tale reclamo sarà inammissibile. In tali occasioni, il Garante richiede all'interessato di allegare al reclamo il documento attestante l'esercizio dei diritti validamente proposto al titolare e la risposta di quest'ultimo.

3. Il principio di accountability

Uno dei temi nuovi, per così dire "trasversali" nella costruzione del Regolamento è certamente il tema dell'"accountability". Si parla di accountability per indicare l'adozione da parte di titolari e responsabili di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione della disciplina stabilita con il Regolamento. Viene in sostanza affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento nel rispetto delle disposizioni normative e dei criteri indicati dal Regolamento.

E' un tema che possiede una complessità intrinseca, tradotto in italiano come "principio di responsabilizzazione", con una traduzione che però non rende in maniera efficace quello che è l'intrinseco significato della parola accountability. Se i principi rimangono gli stessi quello che è nuovo è passare dalla forma alla sostanza. L'art. 5, paragrafo 2, del Regolamento che richiama il concetto espresso dal considerando 74, stabilisce che il titolare è competente per il rispetto dei principi che abbiamo nominato innanzi ed è in grado di comprovarlo. Quindi la vera novità è: non basta più solo essere conforme e rispettare le regole e i principi ma è necessario mettersi nelle condizioni di dimostrare di averli rispettati. Quando parliamo di accountability è come se coniugassimo il verbo "dimostrare" (provare una verità con un procedimento logico o con prove di fatto).

E' un impatto forte dal punto di vista sia tecnico che organizzativo. Corrisponde ad una nuova filosofia del trattamento dei dati. Contribuisce ad nuova cultura dei dati personali. Ma non è un principio che cade all'improvviso. Possiamo ritrovarlo nel parere n. 3/2010 del Gruppo Art. 29 che ne descrive la genesi, come si è arrivati a questa nuova prospettiva, sottolineando che l'obbligo comprende sia l'attuare le misure, sia conservarne le prove. E allora la novità non sta tanto nel principio in sé dell'accountability, ma nel fatto che l'accountability garantisce l'effettività di principi esistenti.

Ma osservare il principio di accountability non dà una presunzione legale di conformità. Il trattamento dei dati poggia su una realtà mutevole in continuo cambiamento, influenzata dal progresso tecnico e tecnologico ed è per questo che ha bisogno di regole flessibili, non si presta a regole statiche, che sarebbero inattuabili. Sta qui la difficoltà e la complicazione della disciplina. Essere accountable non vuol dire essere conforme al Regolamento, ma è un criterio di attenuazione della responsabilità.

4. Privacy by default *e by* design*, registro dei trattamenti, valutazione d'impatto, DPO e* data breach

Come si traduce il principio di *accountability* all'interno del Regolamento?

Il primo dei criteri indicati nel Regolamento riconducibili al principio di accountability è sintetizzato nell'espressione inglese data protection by default e by design che significa: necessità di configurare il trattamento prevedendo sin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati; tenendo conto del contesto complessivo in cui si colloca il trattamento e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento, richiedendo pertanto un'analisi preventiva ed un impegno che deve concretizzarsi in una serie di attività specifiche e dimostrabili. Altro criterio individuato nel Regolamento è quello del rischio inerente il trattamento. Quest'ultimo va inteso quale rischio di impatti negativi sulle libertà e i diritti degli interessati. Tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti e delle misure tecniche e organizzative che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di tale valutazione, il titolare potrà decidere se iniziare il trattamento ovvero consultare l'Autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; in tal caso l'Autorità non avrà il compito di autorizzare il trattamento, ma di indicare le misure ulteriori eventualmente da implementare e potrà adottare le misure correttive (dall'ammonimento, alla limitazione, al divieto del trattamento). L'intervento dell'Autorità di controllo sarà ex post, si porrà, dunque, in un momento successivo alle determinazioni del titolare; ciò spiega il venir meno di istituti quali il prior checking (procedimento di verifica preliminare) sostituito dalla tenuta del registro dei trattamenti e dall'effettuazione della valutazione di impatto da parte del titolare. Peraltro, all'EDPB (Comitato europeo per la protezione dei dati personali) spetterà un ruolo fondamentale al

fine di garantire uniformità di approccio e di fornire ausili interpretativi attraverso la produzione di linee guida e documenti di indirizzo anche per garantire quegli adattamenti necessari alla luce dello sviluppo tecnologico.

Tutti i titolari e i responsabili del trattamento, eccettuati gli organismi con meno di 250 dipendenti e purché non effettuino trattamenti rischiosi, sono tenuti alla redazione di un registro dei trattamenti i cui contenuti sono precisati dal Regolamento (art. 30); si tratta di uno strumento fondamentale allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione o analisi del rischio. Non è solo un adempimento formale, ma è parte integrante di un sistema di corretta gestione dei dati personali.

Tutti i titolari dovranno notificare al Garante le violazioni dei dati personali (data breach) di cui vengono a conoscenza entro 72 ore, ma solo se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Pertanto anche la notifica non è un adempimento obbligatorio, ma sarà subordinata alla valutazione del rischio che spetta al titolare.

Anche la designazione del Responsabile della protezione dei dati (DPO) riflette l'approccio responsabilizzante che è proprio del Regolamento, essendo finalizzata a facilitare l'attuazione del Regolamento da parte del titolare. Tra i compiti del DPO rientrano infatti la sensibilizzazione e la formazione del personale e la sorveglianza sullo svolgimento della valutazione di impatto.

5. Problematiche aperte

Alcuni nodi interpretativi sono attualmente oggetto di un faticoso lavoro di interpretazione da parte dell'Autorità oltreché di condivisione a livello europeo e se ne offre un breve accenno.

In particolare, l'utilizzo dei dati biometrici. Il nuovo assetto regolamentare ha un'impostazione molto rigida e garantista. E fin d'ora appare problematico, soprattutto nel settore privato, l'utilizzo di questi dati, fortemente legati all'implementazione delle misure tecnologiche.

Altro tema delicato e denso di punti critici è il tema delle sanzioni. Molto se ne è parlato specie con riferimento all'astratta previsione di massimi edittali molto elevati. L'Autorità si sta confrontando con le prime applicazioni concrete mentre i profili di maggiore criticità sono dettati dalla necessità, da un lato, di condividere criteri applicativi uniformi con tutti gli Stati membri e, dall'altro lato, di coniugarli con quei principi propri della nostra tradizione giuridica quali il principio di tassatività, certezza, procedimentalizzazione, propri dell'apparato sanzionatorio penale.

Infine, i big data sono considerati oggi il motore dell'economia digitale, definiti anche il petrolio del XXI secolo, non tanto per il potenziale valore del singolo dato, quanto per la possibilità di elaborare, organizzare, analizzare i dati nel loro complesso, attraverso l'utilizzo di software e algoritmi, i quali possono di volta in volta generare un'informazione diversa da quella di partenza, la quale dà a chi la possiede un enorme

vantaggio economico. Attualmente, gli strumenti giuridici messi in atto dal nostro ordinamento non sembrerebbero in grado di tutelare i big data ed i risultati che sono diretta conseguenza dell'elaborazione degli stessi. Ciò potrebbe comportare l'irrigidimento della libertà di circolazione dei dati e il mancato sviluppo dell'economia digitale.

6. La dimensione etica della protezione dei dati personali

Con il nuovo Regolamento, il bilanciamento tra il legittimo interesse dei titolari e i diritti degli interessati non spetta più all'Autorità ma allo stesso titolare, il quale potrà certamente fare riferimento ai provvedimenti di verifica preliminare emanati dal Garante.

Questo dimostra come il principio di accountability informa tutta l'architettura del nuovo Regolamento. Allora potremmo chiederci: qual è il cambiamento? Il vero cambiamento non è il Regolamento, il Regolamento è, in realtà, l'effetto del cambiamento.

C'è una tradizionale sinergia tra la protezione dei dati personali e l'evoluzione tecnologica. La protezione dei dati personali nasce per effetto e per l'impatto dell'evoluzione tecnologica. Sin dal 1800 rincorre l'evoluzione tecnologica e proprio oggi verifichiamo costantemente come sia difficile per la normativa tenere il passo con i cambiamenti tecnologici, mentre siamo esposti a trattamenti privi di categorie giuridiche di riferimento.

La protezione dei dati, seppur intesa qualche volta come un intralcio, può rappresentare, tuttavia, l'ultimo importante momento di riflessione prima di cliccare, prima di rendere possibile la condivisione delle nostre informazioni con una serie indefinita di soggetti.

Un sociologo tedesco, Ulrick Beck, ha detto che l'evoluzione tecnologica va di pari passo con la produzione dei rischi. Il Regolamento introduce garanzie in grado di far fronte ai rischi che da tale evoluzione ne possono derivare, contribuendo a rendere più consapevole l'interessato delle modalità di trattamento dei suoi dati personali (il diritto di accesso è stato ampliato nel suo contenuto, è stato previsto l'obbligo di fornire all'interessato anche informazioni relative all'esistenza di processi decisionali automatizzati come la profilazione).

E in questo senso sicuramente un passo importante è stato fatto dal Regolamento. Lo stesso Tim Cook, CEO di Apple, ha sottolineato il ruolo imprescindibile della regolamentazione dei dati personali.

Prevedere un sistema di regole comuni e uniformi a tutti i Paesi dell'Unione è determinante al fine di colmare lo squilibrio che Buttarelli ha chiamato "Dividendo digitale" ponendo l'attenzione su un modello economico fondato sulla fornitura di servizi gratuiti forniti alle persone in cambio dei loro dati. Il che ha creato un monopolio delle grandi aziende (Microsoft, Apple, Facebook, Google) che non ha eguali.

Nel tentativo di ristabilire un equilibrio tra posizioni fortemente squilibrate a vantaggio dei grandi colossi del tech, l'obiettivo è quello di tendere ad uno sviluppo

economico ed etico sostenibile, di ricercare la dimensione etica dello sviluppo tecnologico, attraverso la valorizzazione della dimensione etica della protezione dei dati personali.

Il Regolamento ha fatto molti passi avanti in questo senso, valorizzando il principio di trasparenza e di finalità. Ma le sanzioni non bastano, è necessario sottolineare il valore del dato personale, favorire una cultura giuridica che ponga al centro il diritto alla privacy, in primo luogo rendendo edotti gli interessati utenti dell'importanza del controllo delle loro informazioni, perché senza accorgersene, regalando i propri dati in cambio di servizi solo apparentemente gratuiti, si troveranno spogliati del potere di decidere, protagonisti di una dittatura digitale in cui le grandi aziende saranno in grado di influenzare i loro comportamenti, le loro abitudini, le loro scelte di vita, finanche le loro opinioni politiche.

Non è vero che più tecnologia corrisponde a più felicità. La tecnologia può fare grandi cose, come produrre grossi danni. Siamo noi che dobbiamo darle un senso, indirizzarla verso ciò che è giusto. Vorrei concludere ricordando un'affermazione di Giovanni Buttarelli: *"Rispettare la legge alla lettera è importante ma non è sufficiente. L'etica viene prima, durante e dopo la legge. Riempie i vuoti lasciati dalla legge. Sfida la legge, e chi la scrive, a migliorare. Un tempo la schiavitù era illegale, ma l'etica è servita a combattere per abolirla. I temi stanno diventando enormi: nella questione dell'etica digitale sono coinvolte le dimensioni fondamentali della democrazia, della giustizia, della concentrazione del potere, della valorizzazione dei dati di ciascuno a vantaggio di persone. Tutte le rivoluzioni fanno delle vittime: dobbiamo rigenerare i valori che servono a guidare la società verso il futuro"*.

Protezione dei dati personali, tutela del consumatore e concorrenza: un rapporto in evoluzione

DI AURORA SAIJA *

SOMMARIO: 1. Introduzione – 2. Alcune nozioni cruciali. – 2.1. Il consenso dell'interessato e i requisiti di validità. – 2.2. La trasparenza del trattamento. – 2.3. La portabilità dei dati – 3. Privacy, concorrenza e tutela del consumatore: implicazioni per il *due process.* – 4. Privacy, concorrenza e tutela del consumatore: la questione dei risarcimenti. – 5. Conclusioni.

1. Introduzione

L'avvento del digitale ha trasformato con una velocità senza precedenti le abitudini di vita e di consumo, i rapporti tra le persone, i modelli di business, e ha messo in luce la centralità della protezione dei dati personali per una crescita economica che sia radicata sul rispetto dei diritti fondamentali dell'individuo. La ricerca di un adeguato contemperamento tra la protezione dei diritti fondamentali e la libertà d'impresa e di prestazione di servizi è essenziale per la realizzazione e lo sviluppo del mercato unico digitale e per la competitività dell'economia europea[1].

In questo scenario, un tema su cui riflettere è quello dell'interazione tra la disciplina in materia di protezione dei dati personali e altri plessi normativi che riguardano l'attività delle imprese e mirano a tutelare beni giuridici diversi dalla privacy, quali la capacità del consumatore di scegliere in modo informato e consapevole o il corretto svolgimento del gioco concorrenziale. Nell'ambito delle varie questioni che il tema solleva, il presente contributo si sofferma su tre aspetti. Il primo attiene all'individuazione degli elementi della normativa sulla protezione dei dati che possono assumere rilievo ai fini dell'applicazione delle disposizioni in materia di tutela del consumatore, con particolare riguardo alle norme sulle pratiche commerciali scorrette, o del diritto antitrust.

Il secondo aspetto è relativo all'attuazione delle garanzie di *due process*, in un quadro giuridico caratterizzato dalla coesistenza di diverse normative in linea di principio applicabili a una data condotta d'impresa e dalla pluralità di autorità pubbliche incaricate dell'accertamento delle violazioni e dell'irrogazione di sanzioni ai soggetti responsabili.

* Responsabile Area attività d'impresa e concorrenza, Assonime.

[1] V. la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale, COM (2017) 228 final.

Il terzo aspetto riguarda il risarcimento del danno causato da un illecito trattamento di dati personali, eventualmente quale presupposto o elemento costitutivo di una diversa infrazione. A valle del GDPR[2] il focus della tutela, e conseguentemente delle pretese risarcitorie fatte valere in sede giudiziale, si va spostando sempre più sul diritto dell'individuo al controllo dei propri dati. Ciò induce a ripensare gli elementi fondanti del sistema della responsabilità civile e i criteri per la determinazione dei danni relativi a dati personali.

2. Alcune nozioni cruciali

2.1. Il consenso dell'interessato e i requisiti di validità

Tra gli elementi della disciplina in materia di privacy destinati ad assumere rilievo nel contesto di altre normative va anzitutto considerato il consenso dell'interessato che, secondo quanto previsto dal GDPR, costituisce una delle possibili basi giuridiche del trattamento di dati personali[3]. L'esperienza recente evidenzia che le condizioni e le modalità con cui un'impresa acquisisce dall'interessato il consenso al trattamento dei dati personali sono oggetto di attenzione crescente da parte delle autorità preposte all'applicazione del diritto antitrust o delle norme che tutelano i consumatori dalle pratiche commerciali scorrette delle imprese.

A questo riguardo, il 'caso Facebook', su cui si sono pronunciate a breve distanza di tempo in Italia l'Autorità garante della concorrenza e del mercato (AGCM) e in Germania il Bundeskartellamt rappresenta un esempio significativo del diverso inquadramento che può essere attribuito a una medesima condotta incentrata su un illecito trattamento di dati personali[4]. Entrambe le autorità hanno, infatti, contestato alla piattaforma di aver acquisito in modo improprio il consenso degli utenti all'utilizzo dei loro dati personali per finalità che esulano dalla prestazione del servizio di social network. Mentre tuttavia l'AGCM ha esercitato la sua competenza in materia di tutela del consumatore, e precisamente in materia di pratiche commerciali scorrette[5], l'autorità tedesca ha agito nei confronti di Facebook applicando le norme a tutela della concorrenza.

L'intervento dell'AGCM si è fondato sulla premessa che il rapporto tra la piattaforma e i suoi iscritti configura un rapporto di consumo in quanto, pur pur in assenza di un corrispettivo monetario, è presente uno 'scambio' tra il servizio di social network offerto dalla prima e l'insieme dei dati personali conferiti dai secondi, che nella moderna economia basata sul digitale hanno un valore economico[6]. Muovendo da questa

[2] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, Regolamento generale sulla protezione dei dati personali – GDPR.
[3] Articolo 6 del GDPR.
[4] Cfr. Autorità garante della concorrenza e del mercato, provvedimento n. 27432 del 29 novembre 2018, e Bundeskartellamt, decisione del 6 febbraio 2019, B6-22/16.
[5] Articoli 18 e ss. del decreto legislativo 6 settembre 2005, n. 206 (Codice del consumo).
[6] Questo approccio era già emerso nel provvedimento AGCM n. 26597 dell'11 maggio 2017 (Whatsapp-Trasferimento dati a Facebook).

prospettiva l'Autorità, oltre ad accertare il carattere ingannevole delle informazioni che Facebook forniva all'utente in fase di attivazione dell'account riguardo alla asserita gratuità del servizio, ha considerato aggressiva mediante indebito condizionamento la pratica consistente nell'indurre l'utente, mediante un meccanismo di preselezione del consenso e la prospettazione di conseguenze pregiudizievoli in caso di diniego (incluse limitazioni alla fruibilità del social network), ad accettare la condivisione di dati personali tra la piattaforma e siti o applicazioni di terze parti. Per ciascuna delle due pratiche scorrette riscontrate l'Autorità ha irrogato a Facebook una sanzione di cinque milioni di euro, che corrisponde al massimo edittale previsto dal Codice del consumo per queste violazioni. Va osservato che in sede di ricorso la decisione dell'AGCM è stata parzialmente annullata dal Tar Lazio, con riferimento alla pratica relativa alla condivisione dei dati dell'utente in assenza di un suo consenso espresso: il Tar ha rilevato vizi nel percorso motivazionale seguito dall'Autorità, in termini sia di non convincente ricostruzione del meccanismo di integrazione delle piattaforme, sia di insufficiente dimostrazione dell'esistenza di una condotta idonea a condizionare le scelte del consumatore[7].

Il Bundeskartellamt si è invece concentrato sull'accertamento della posizione dominante detenuta da Facebook nel mercato dei social network e ha qualificato come abuso di posizione dominante ai sensi del diritto antitrust la condotta dell'impresa consistente nell'aver acquisito, aggregato ed elaborato a scopi di profilazione informazioni provenienti da molteplici fonti e applicazioni senza un valido consenso dell'utente. Secondo questo approccio, la violazione della normativa sulla protezione dei dati personali costituisce una manifestazione del potere di mercato dell'impresa. L'Autorità tedesca non ha irrogato sanzioni, limitandosi a imporre a Facebook la modifica della policy in materia di trattamento dei dati degli utenti. La decisione è stata successivamente sospesa in sede cautelare dalla Corte d'appello di Dusseldorf, che non ha condiviso la valutazione per cui un trattamento di dati personali non conforme alla normativa sulla privacy posto in essere da un'impresa in posizione dominante possa costituire un abuso ai sensi del diritto antitrust[8]. Chiamata a esprimersi sulla questione, la Corte di cassazione tedesca (Bundesgerichtshof) ha annullato la sospensiva disposta dalla Corte d'appello, ponendo l'enfasi sull'impatto restrittivo della concorrenza della condotta di Facebook in termini di riduzione della scelta del consumatore[9].

Tenuto conto di questi orientamenti, conviene soffermarsi sulle prescrizioni relative al consenso contenute nel GDPR, che sono suscettibili di assumere rilievo ai fini della valutazione di una condotta d'impresa in una prospettiva di tutela del consumatore o della concorrenza[10].

[7] Tar Lazio, 10 gennaio 2020, n. 261.
[8] Oberlandsgericht Düsseldorf, 26 agosto 2019, VI-Kart 2/19 (V).
[9] Cfr. il comunicato stampa del 23 giugno 2020 sul sito https://juris.bundesgerichtshof.de.
[10] Peraltro, è stato evidenziato che con riferimento alla gestione dei Big Data il sistema dell'acquisizione del consenso dell'interessato disciplinato dal GDPR presenta delle criticità in

Com'è noto, il GDPR definisce il consenso come manifestazione di volontà libera, specifica, informata e inequivocabile[11]; l'ampia prassi decisionale del Garante nazionale e le Linee guida del Comitato europeo per la protezione dei dati[12] (EDPB) forniscono un importante ausilio nell'interpretazione dei requisiti di validità del consenso.

In particolare, con riferimento al carattere inequivocabile del consenso la normativa indica la necessità di un comportamento attivo che attesti l'accettazione del trattamento ad opera dell'interessato e preclude il ricorso a tecniche di preimpostazione[13]. Più problematica, soprattutto nel contesto digitale, può essere la questione di come assicurare che il consenso sia pienamente informato, per la difficoltà di accertare che le informazioni fornite dal titolare siano state effettivamente acquisite e comprese dall'interessato, e libero, nel senso che l'interessato non deve aver subito pressioni o coercizioni, anche in forma di prospettazione di conseguenze negative – che, come chiarito dall'EDPB, devono essere 'significative' – a cui si troverebbe esposto per l'eventuale diniego o revoca del consenso.

Una fattispecie controversa è quella del cosiddetto *bundling* o condizionalità, che consiste nel subordinare l'esecuzione di un contratto o la prestazione di un servizio al rilascio del consenso a un trattamento di dati ulteriore, non necessario per l'esecuzione del contratto stesso. Il GDPR dispone che questa pratica deve essere tenuta 'nella massima considerazione' quando si valuta se il consenso è stato prestato liberamente[14]. Il Comitato europeo di protezione dei dati, nelle Linee guida in materia di consenso sopra richiamate, ha aderito a un approccio molto restrittivo, secondo il quale dal GDPR deriverebbe con riferimento al *bundling* una presunzione forte di mancanza di libertà del consenso. Per superarla, il titolare del trattamento dovrebbe riuscire a dimostrare di aver messo l'interessato in grado di scegliere tra un servizio che prevede il consenso al trattamento di dati per finalità ulteriori e un servizio equivalente, offerto dallo stesso titolare, che non implica tale consenso.

L'onere probatorio che viene così posto in capo al titolare del trattamento appare eccessivamente gravoso. Secondo un'impostazione più flessibile e coerente con il principio di proporzionalità, nei casi di *bundling* il titolare dovrebbe avere la possibilità di dimostrare la libertà del consenso tenendo conto di elementi quali la natura del prodotto

quanto tali dati «sono di sovente trattati per scopi determinati solo in termini generali; le finalità non vengono, in realtà, specificamente individuate *ex ante*, in ragione dell'emersione delle correlazioni fra i dati solo in fase successiva alla raccolta degli stessi». Cfr. Autorità garante della concorrenza e del mercato, Autorità per le garanzie nelle comunicazioni, Garante per la protezione dei dati personali (2020), *Indagine Conoscitiva sui Big Data*, p. 25.

[11] Articolo 4, n. 11, del GDPR.

[12] Linee guida 5/2020 del Comitato europeo per la protezione dei dati (EDPB) in materia di consenso.

[13] Il considerando 32 del GDPR indica quali possibili modalità per l'espressione del consenso la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto, e sottolinea che non dovrebbero configurare consenso il silenzio, l'inattività o la preselezione di caselle.

[14] Articolo 7, paragrafo 4, del GDPR.

o servizio, le alternative disponibili sul mercato per l'interessato, il tipo di trattamento e di dati coinvolti, l'assenza di un impatto apprezzabile sulla sfera individuale, la completezza e la chiarezza delle informazioni rese all'interessato.

Sul punto merita di essere ricordata l'interpretazione che emerge da una pronuncia della Corte di Cassazione relativa a un caso in cui il consenso dell'interessato costituiva condizione per fruire di un servizio di newsletter via email e i dati acquisiti attraverso l'iscrizione alla newsletter erano utilizzati dal gestore del sito anche per l'invio di comunicazioni commerciali[15]. La Corte ha sostenuto che il condizionamento «non possa sempre e comunque essere dato per scontato e debba invece essere tanto più ritenuto sussistente, quanto più la prestazione offerta dal gestore del sito Internet sia ad un tempo infungibile ed irrinunciabile per l'interessato»; in presenza di un servizio né infungibile né irrinunciabile, nulla impedisce al gestore del sito, secondo la Corte, di negare il servizio offerto a chi non si presti a ricevere messaggi promozionali[16].

2.2. La trasparenza del trattamento

Un secondo elemento del regime in materia di protezione dei dati personali che può essere valutato anche in una prospettiva di concorrenza o tutela del consumatore è quello relativo alle informazioni da rendere all'interessato e, più in generale, alla trasparenza del trattamento. È stato osservato che tali informazioni «vanno ad integrare esse stesse una componente "concorrenziale" rispetto al trattamento posto in essere dai singoli titolari del trattamento, ben potendo orientare (nell'ipotesi in cui il trattamento acceda ad un'offerta di beni o servizi, le scelte di quanti vedono le informazioni a sé riferite coinvolte nel trattamento (così dando attuazione al diritto all'autodeterminazione informativa), non diversamente dalle informazioni contenute sulle etichette e dai documenti informativi che i consumatori consultano prima di procedere all'acquisto di beni di consumo»[17].

Anche questo profilo è stato oggetto di contestazioni nei confronti di Facebook, da parte sia dell'AGCM, che ha censurato l'omissione di informazioni sulle finalità remunerative perseguite dalla piattaforma mediante l'utilizzo dei dati personali degli iscritti[18], sia del Bundeskartellamt, secondo cui l'inadeguatezza delle informazioni sulla

[15] Corte di Cassazione, 2 luglio 2018, n. 17278.

[16] La Corte ha quindi escluso che un generico servizio informativo, quale quello del caso di specie, costituisca una prestazione infungibile e irrinunciabile per l'interessato, tenuto conto che «all'evidenza si tratta di informazioni agevolmente acquisibili per altra via, eventualmente attraverso siti a pagamento, se non attraverso il ricorso all'editoria cartacea, con la conseguenza che ben può rinunciarsi a detto servizio senza gravoso sacrificio». La stessa sentenza sottolinea che «l'ordinamento non vieta lo scambio di dati personali, ma esige tuttavia che tale scambio sia frutto di un consenso pieno ed in nessun modo coartato»

[17] Indagine conoscitiva sui Big Data, cit., p. 58.

[18] Secondo l'Autorità, l'informazione in merito alla raccolta e all'utilizzo, a fini remunerativi, dei dati dell'utente e, conseguentemente dell'intento commerciale perseguito, volto alla monetizzazione dei medesimi, è un'informazione rilevante di cui il consumatore necessita al fine di assumere una decisione consapevole di natura commerciale quale è quella di registrarsi nella piattaforma per usufruire del servizio di social network.

combinazione automatica dei dati raccolti avrebbe comportato l'invalidità dei consensi acquisiti, dando luogo alla condotta abusiva.

Il GDPR ha rafforzato gli obblighi di trasparenza e completezza delle informazioni con riferimento ai trattamenti di dati che avvengono nel contesto digitale. Si consideri, in particolare, che il titolare del trattamento è tenuto a informare l'interessato anche dell'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione, e a fornirgli informazioni significative sulla logica utilizzata, nonché sull'importanza e le previste conseguenze di tale trattamento[19]. Come indicato in un documento del Gruppo di lavoro Articolo 29 (oggi sostituito dall'EDPB), le informazioni devono essere «sufficientemente complete affinché l'interessato possa comprendere i motivi alla base della decisione»[20]. La sfida, per le imprese che operano sul web attraverso processi decisionali automatizzati, è quella di riuscire a rendere comprensibile la logica degli algoritmi utilizzati.

2.3. La portabilità dei dati

Un'altra nozione che si colloca al crocevia tra protezione dei dati personali, concorrenza e tutela del consumatore-utente di servizi digitali è quella di portabilità dei dati. Il GDPR ha introdotto il diritto dell'interessato a ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati forniti a un titolare del trattamento e trasmetterli, senza impedimenti, ad altro titolare oppure ottenerne la trasmissione diretta dal titolare originario al nuovo titolare[21]. Questo diritto si applica con riferimento ai trattamenti che hanno come base giuridica il consenso preventivo dell'interessato o un contratto e sono effettuati con mezzi automatizzati.

Secondo una visione largamente condivisa, la portabilità rappresenta la massima espressione del diritto dell'interessato al controllo dei propri dati personali. Allo stesso tempo, consentendo il passaggio dell'utente da un fornitore all'altro, è uno strumento per favorire la concorrenza e l'innovazione nel mercato dei servizi digitali e promuovere l'interoperabilità delle piattaforme.

Da ciò discende anzitutto l'esigenza di definire con chiarezza l'ambito di applicazione della previsione, individuando quali dati sono suscettibili di portabilità. L'orientamento delle autorità europee di protezione dei dati è nel senso che il diritto riguardi sia i dati direttamente forniti dall'interessato, sia i dati risultanti dall'osservazione della sua attività nel contesto digitale[22]. Restano tuttavia margini di incertezza per quanto riguarda, nei casi concreti, la distinzione tra dati forniti dall'interessato e dati che sono frutto di una autonoma elaborazione del titolare[23].

[19] Articolo 13, par. 2, lett. f, del GDPR.
[20] Gruppo di lavoro Art. 29, WP251 rev. 01., *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.*
[21] Articolo 20 del GDPR.
[22] Gruppo di lavoro Art. 29, WP242 rev. 01, *Guidelines on the Right to data portability*.
[23] Cfr. Indagine conclusiva sui Big Data, cit., p. 98.

Inoltre, per l'attuazione della norma è indispensabile lo sviluppo di standard aperti e formati interoperabili che consentano la trasmissione e il riutilizzo dei dati in un sistema sempre più interconnesso.

3. Privacy, concorrenza e tutela del consumatore: implicazioni per il due process

Passando dalla prospettiva sostanziale a quella procedurale, è evidente come l'interferenza tra i diversi plessi normativi e la tendenza delle autorità pubbliche a istruire procedimenti in campo antitrust o in materia di pratiche commerciali scorrette sulla base di asserite violazioni delle norme sulla protezione dei dati personali porta a interrogarsi sul possibile conflitto di competenze, sui rischi di *bis in idem* e sulle conseguenze che discendono sul piano sanzionatorio dal tipo di intervento che viene realizzato.

Va considerato che i sistemi di *enforcement* presentano significative differenze, sia per quanto riguarda i poteri di indagine e gli strumenti a disposizione delle autorità (si pensi alle decisioni con impegni)[24], sia con riferimento alle sanzioni irrogabili nel caso di accertamento di una violazione[25]. Peraltro, a seconda della normativa applicata e dell'autorità procedente, può essere diverso anche il giudice del ricorso: in Italia, le decisioni adottate dall'AGCM tanto in materia antitrust quanto di pratiche commerciali scorrette sono impugnabili davanti al giudice amministrativo, mentre i provvedimenti del Garante privacy sono impugnabili davanti al giudice ordinario.

Nel caso Facebook, l'eccezione di incompetenza dell'AGCM in favore del Garante privacy è stata respinta sulla base del rilievo che le due normative in gioco hanno un campo di applicazione materiale differente e perseguono interessi distinti (diritto fondamentale della persona alla protezione dei suoi dati vs. tutela della libertà di scelta del consumatore), risultando pertanto complementari. Questa impostazione è stata avallata dal giudice amministrativo. Il Tar ha peraltro osservato che non esiste «il paventato rischio di un effetto plurisanzionatorio della medesima condotta (intesa come identico fatto storico)» in quanto «l'oggetto di indagine da parte delle competenti autorità

[24] Si tratta delle decisioni con cui un'autorità accetta e rende vincolanti gli impegni proposti dalle imprese per rimuovere i profili problematici della condotta oggetto d'istruttoria, senza giungere all'accertamento dell'infrazione: nel nostro ordinamento l'AGCM ha il potere di adottare queste decisioni sia in materia antitrust (cfr. l'articolo 14-*ter* della legge n. 287/1990) che di tutela del consumatore (cfr. l'articolo 27, comma 7, del Codice del consumo), mentre il Garante privacy non dispone di questo strumento.

[25] In particolare: le sanzioni per le violazioni del diritto antitrust possono raggiungere il 10% del fatturato totale realizzato a livello mondiale dalle imprese; per le violazioni in materia di protezione dei dati il GDPR prevede sanzioni fino al 4% del fatturato mondiale totale delle imprese; per le pratiche commerciali scorrette l'AGCM può attualmente irrogare sanzioni fino a 5 milioni di euro. Va però osservato che la recente direttiva (UE) 2019/2161 del Parlamento europeo e del Consiglio, del 27 dicembre 2019, che dovrà essere recepita entro il 28 novembre 2021, dispone che per varie infrazioni in materia di protezione dei consumatori, comprese le pratiche commerciali scorrette, le autorità degli Stati membri possano irrogare sanzioni fino a un importo massimo almeno pari al 4% del fatturato annuo realizzato dall'impresa nello Stato membro o negli Stati membri interessati.

riguarda condotte differenti dell'operatore, afferenti in un caso al corretto trattamento del dato personale ai fini dell'utilizzo della piattaforma, nell'altro caso alla chiarezza e completezza dell'informazione circa lo sfruttamento del dato ai fini commerciali».

La questione appare comunque controversa e suscettibile di produrre incertezze. Un'applicazione parallela delle discipline da parte delle due autorità competenti in relazione a situazioni concrete in cui non è chiara la differenza tra le condotte contestate si traduce di fatto per l'impresa nel rischio di subire un doppio procedimento e una duplice condanna, in contrasto con il principio sancito dall'articolo 4 del Protocollo n. 7 della Convenzione europea dei diritti dell'uomo e dall'articolo 50 della Carta europea dei diritti fondamentali. Va ricordato che, secondo la giurisprudenza della Corte EDU, ai fini dell'applicazione del principio del *ne bis in idem* non occorre l'identità della qualificazione giuridica o dell'interesse tutelato: l'*idem* ricorre quando vi è coincidenza dei fatti e del soggetto a cui è imputata la violazione[26]. La Corte ha inoltre chiarito che la violazione del principio può essere esclusa nel caso di procedimenti che presentano una stretta connessione sostanziale e temporale, a condizione che essi risultino coordinati sul piano istruttorio, mediante forme di circolazione della prova e con adeguate garanzie, e sul piano sanzionatorio, nel senso che la sanzione complessivamente inflitta deve essere proporzionata[27].

Per favorire l'interazione tra le autorità e prevenire eventuali conflitti nell'applicazione delle varie normative nel contesto digitale, a livello UE il Garante europeo per la protezione dei dati ha promosso l'istituzione di un foro di discussione, denominato Digital Clearinghouse, a cui partecipano su base volontaria le autorità di concorrenza, le autorità di tutela dei consumatori e i garanti della privacy degli Stati membri.

A livello di singoli ordinamenti nazionali la situazione è eterogenea. Con riferimento ai casi Facebook sopra menzionati, mentre in Germania il Bundeskartellamt ha stabilito uno stretto contatto con le autorità di protezione dei dati personali nel corso del procedimento, in Italia non risultano esservi stati analoghi tentativi di interlocuzione tra AGCM e Garante privacy.

La cooperazione tra le autorità può fornire un contributo importante alla certezza giuridica e alla coerenza del sistema e andrebbe promossa con impegno. Sarebbe, ad esempio, buona prassi che l'AGCM chiedesse il parere del Garante privacy nel procedimento di applicazione della normativa sulle pratiche commerciali scorrette a fattispecie basate su un illecito trattamento di dati, in linea con quanto previsto dal Codice del consumo con riferimento ai rapporti tra AGCM e autorità di regolazione settoriale[28].

Un impulso al rafforzamento della cooperazione può venire oggi dal Regolamento (UE) 2017/2394, che disciplina il funzionamento della rete delle autorità responsabili dell'esecuzione della normativa a tutela dei consumatori (c.d. Regolamento CPC,

[26] Cfr. Corte europea dei diritti dell'uomo, 10 febbraio 2009, *Sergey Zolotukhin c. Russia*, e 17 febbraio 2015, *Boman c. Finlandia.*
[27] Corte europea dei diritti dell'uomo (Grande Camera), 15 novembre 2016, *A e B c. Norvegia*.
[28] Articolo 27, comma 1-*bis*, del Codice del consumo.

Consumer protection cooperation) ed è applicabile dal 17 gennaio 2020. Il sistema CPC è stato istituito per favorire il contrasto alle infrazioni delle norme europee a tutela degli interessi dei consumatori aventi una dimensione transfrontaliera. Ciascuno Stato deve designare una o più autorità pubbliche che partecipano alla rete e sono quindi tenute a collaborare fra loro e con la Commissione europea per garantire il rispetto delle norme a tutela dei consumatori, indicate in un allegato al Regolamento, e il buon funzionamento del mercato interno, nonché migliorare la tutela degli interessi economici dei consumatori. Nel caso di pluralità di autorità competenti, lo Stato deve garantire che le loro rispettive funzioni siano chiaramente definite e che operino in stretta collaborazione. Per l'Italia sono incluse nell'elenco delle autorità designate sia l'AGCM sia il Garante privacy[29].

4. Privacy, concorrenza e tutela del consumatore: la questione dei risarcimenti[30]

Un'ultima dimensione interessante del rapporto tra discipline di fonti diverse e della possibile pluralità di interventi sanzionatori è quella relativa all'applicazione delle norme da parte del giudice in sede di controversie tra privati. A seconda della violazione accertata, dell'autorità procedente e del modo in cui si è concluso il procedimento possono esservi ripercussioni diverse sul piano del *private enforcement*.

Si consideri in particolare il profilo dell'effetto delle decisioni amministrative sui successivi giudizi risarcitori: mentre per la constatazione di infrazioni antitrust da parte di un'autorità di concorrenza è espressamente prevista un'efficacia vincolante nelle azioni risarcitorie *follow-on*[31], per i provvedimenti che accertano pratiche commerciali

[29] L'AGCM risulta designata quale autorità competente con riferimento ai seguenti atti legislativi europei: Direttiva 2000/31/CE sul commercio elettronico, Direttiva 2005/29/CE sulle pratiche commerciali sleali, Direttiva 2006/114/CE sulla pubblicità ingannevole e comparativa, Direttiva 2006/123/CE sui servizi nel mercato interno, Direttiva 2011/83/UE sui diritti dei consumatori, Direttiva 2013/11/UE sull'ADR per i consumatori, Direttiva 93/13/CEE sulle clausole abusive nei contratti con i consumatori, Regolamento (UE) 2018/302 sul *geoblocking*, Regolamento (UE) n. 524/2013 sull'ODR per i consumatori. Il Garante per la protezione dei dati personali risulta designato con riferimento alla Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, c.d. Direttiva e-privacy (cfr. l'elenco degli uffici unici di collegamento e delle autorità competenti designati dagli Stati membri pubblicato sul sito della Commissione europea).

[30] Regolamento (UE) 2017/2394 del Parlamento europeo e del Consiglio del 12 dicembre 2017 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori e che abroga il regolamento (CE) n. 2006/2004.

[31] Cfr. la Direttiva 2014/104/UE del Parlamento europeo e del Consiglio, del 26 novembre 2014, relativa a determinate norme che regolano le azioni per il risarcimento del danno ai sensi del diritto nazionale per violazioni delle disposizioni del diritto della concorrenza degli Stati membri e dell'Unione europea, il cui articolo 9, par. 1, richiede agli Stati membri di provvedere affinché una violazione del diritto della concorrenza constatata da una decisione definitiva di un'autorità nazionale della concorrenza o di un giudice del ricorso sia ritenuta definitivamente accertata ai fini dell'azione per il risarcimento del danno proposta dinanzi ai loro giudici nazionali ai sensi delle norme antitrust europee o nazionali. L'articolo 7 del decreto legislativo 19 gennaio 2017, n. 3, di attuazione della Direttiva 2014/104/UE nell'ordinamento italiano, ha previsto che ai fini

scorrette o violazioni della disciplina sulla protezione dei dati personali non vi sono ad oggi disposizioni che stabiliscano un particolare valore probatorio[32]. Va osservato che la proposta di direttiva sulle azioni rappresentative a tutela degli interessi collettivi dei consumatori, presentata dalla Commissione europea nell'aprile 2018, prevedeva l'effetto vincolante delle decisioni di accertamento delle violazioni di un ampio insieme di norme dell'Unione volte alla tutela del consumatore, elencate nell'Allegato I, comprese le norme della direttiva sulle pratiche commerciali scorrette e le norme del GDPR[33]. Tuttavia, il testo su cui è stato raggiunto l'accordo segue un approccio meno radicale, che accorda alla decisione di accertamento della violazione un valore probatorio semplice, definito in conformità alla normativa del singolo Stato membro in tema di valutazione della prova[34].

In ogni caso, anche qualora la decisione amministrativa abbia efficacia nelle azioni risarcitorie *follow-on*, resta fermo per chi agisce in giudizio l'onere di provare l'esistenza del danno subito e il nesso causale e di quantificare il danno.

Riguardo al primo aspetto, una questione che emerge in relazione alla possibile interferenza tra varie norme è se il danno risarcibile può avere una diversa configurazione a seconda che l'azione risarcitoria verta su una violazione antitrust, oppure su una violazione della normativa in tema di pratiche commerciali scorrette (sia pure basate su un illecito trattamento di dati personali), oppure sulla mera non conformità di una condotta d'impresa alla disciplina in materia di privacy.

Va considerato che nel caso di illeciti antitrust e di pratiche commerciali scorrette il danno ha tipicamente natura economica. Per le violazioni in materia di privacy il discorso è in linea di principio diverso, in quanto il pregiudizio riguarda la sfera più intima della persona.

---

dell'azione per il risarcimento del danno, si ritiene definitivamente accertata, nei confronti dell'autore, la violazione del diritto della concorrenza constatata da una decisione dell'AGCM non più soggetta ad impugnazione davanti al giudice del ricorso, o da una sentenza del giudice del ricorso passata in giudicato.

[32] La Corte di Cassazione ha recentemente chiarito che «il provvedimento del Garante per la protezione dei dati personali, che abbia accertato l'illegittimità della raccolta e della diffusione di determinati dati personali (…) mai può acquistare un'efficacia (equiparabile a quella) di cosa giudicata nel separato giudizio che l'interessato abbia successivamente instaurato, dinanzi all'autorità giudiziaria ordinaria, per ottenere il risarcimento dei danni asseritamente provocatigli dalla lesione del diritto alla riservatezza ed alla protezione di quei dati atteso che la natura amministrativa dell'organo e del relativo procedimento non pone il Garante in una posizione di terzietà assimilabile a quella assicurata dal giudice nel processo» (Corte di Cassazione, 25 maggio 2017, n. 13151).

[33] COM (2018) 184 final.

[34] Cfr. l'articolo 10 del testo approvato dal Comitato dei rappresentanti permanenti degli Stati membri (Coreper) il 30 giugno 2020: "*Member States shall ensure that a final decision of a court or an administrative authority of any Member State on the existence of an infringement harming collective interests of consumers can be used by both parties as evidence in the context of any other actions seeking redress before their national courts or administrative authorities against the same trader for the same infringement, in accordance with national law on evaluation of evidence*".

Nel nostro ordinamento, esiste un consolidato orientamento della giurisprudenza secondo cui la lesione del diritto alla privacy comporta un danno non patrimoniale, poiché investe interessi inerenti la persona non connotati da rilevanza economica. Ad esempio, in una recente pronuncia la Cassazione ha affermato che deve essere riconosciuta nella generalità dei consociati la sussistenza di un «intimo desiderio/necessità di riservatezza», costituente «il principale dei valori che le norme sulla privacy riconoscono ed intendono tutelare»[35]. Il danno deve naturalmente essere allegato e provato in quanto, come chiarito dalla stessa Cassazione, «non si identifica nell'evento dannoso – cioè nell'illecito trattamento dei dati personali – ma deve concretizzarsi in un pregiudizio della sfera non patrimoniale di interessi del danneggiato»[36].

Al danno connesso alle violazioni in materia di privacy si applicano quindi i criteri dettati in generale dalla nota sentenza delle Sezioni Unite della Cassazione n. 26972/2008 sul danno non patrimoniale, che infatti richiama tra le ipotesi di risarcimento del danno non patrimoniale espressamente previste nel nostro ordinamento quella relativa all'impiego di modalità illecite nella raccolta di dati personali[37]. Conviene ricordare che, secondo le indicazioni della Cassazione, la lesione deve essere seria (non futile o irrisoria) e il danno deve essere grave e dunque eccedere una certa soglia minima. Questo duplice filtro «attua il bilanciamento tra il principio di solidarietà verso la vittima, e quello di tolleranza, con la conseguenza che il risarcimento del danno non patrimoniale è dovuto solo nel caso in cui sia superato il livello di tollerabilità ed il pregiudizio non sia futile. Pregiudizi connotati da futilità ogni persona inserita nel complesso contesto sociale li deve accettare in virtù del dovere della tolleranza che la convivenza impone (art. 2 Cost.)». Questi requisiti sono stati richiamati in varie successive pronunce della Cassazione che riguardano specificamente il danno non patrimoniale nel caso di violazioni in materia di privacy[38].

Il tema della situazione giuridica protetta e del danno risarcibile ha acquisito tuttavia, a valle del GDPR, una nuova prospettiva. Il GDPR ha segnato infatti l'emergere del diritto dell'individuo al controllo dei propri dati personali, risultante in particolare dalla previsione sopra menzionata che assicura la portabilità dei dati[39]. Ciò determina un'importante evoluzione rispetto all'impostazione tradizionale in cui oggetto della tutela

[35] Corte di Cassazione, 13 febbraio 2018, n. 3426.
[36] Corte di Cassazione, 5 settembre 2014, n. 18812.
[37] Corte di Cassazione, SS.UU., 11 novembre 2008, n. 26972.
[38] Cfr. ad esempio Corte di Cassazione, 15 luglio 2014, n. 16133, e 8 febbraio 2017, n. 3311, secondo cui «il danno non patrimoniale risarcibile ai sensi del codice della privacy, pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali tutelato dagli artt. 2 e 21 Cost. e dall'art. 8 della CEDU, non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno" (quale perdita di natura personale effettivamente patita dall'interessato), in quanto anche per tale diritto opera il bilanciamento con il principio di solidarietà ex art. 2 Cost., di cui il principio di tolleranza della lesione minima è intrinseco precipitato, sicché determina una lesione ingiustificabile del diritto non la mera violazione delle prescrizioni poste dall'art. 11 del medesimo codice ma solo quella che ne offenda in modo sensibile la sua portata effettiva».
[39] Cfr. l'articolo 20 del GDPR.

era esclusivamente il diritto, fondamentale e inviolabile, al rispetto della vita privata e alla riservatezza.

Coerentemente, il considerando 85 del GDPR chiarisce che «una violazione dei dati personali può (…) provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita di controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione di identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata».

In alcuni Stati membri sono state esperite con successo negli ultimi anni azioni individuali risarcitorie per la lesione del diritto al controllo dei dati personali causata da una condotta in violazione della normativa privacy; il danno riconosciuto è di tipo immateriale, talvolta rapportato alla situazione di ansia e stress patita dal singolo soggetto.

Recentemente inoltre si osserva in Europa la diffusione di azioni collettive contro i grandi operatori del digitale, nelle quali viene chiesto il diritto al risarcimento del danno in termini di perdita di controllo dei dati personali causato a una molteplicità di individui da condotte non conformi alla disciplina in materia di privacy. A questo riguardo, si possono trarre interessanti spunti di riflessione dalle pronunce dei giudici inglesi in ordine all'ammissibilità dell'azione di classe Lloyd contro Google, nella quale viene chiesto il risarcimento per una raccolta di dati personali effettuata, secondo l'attore, in modo non conforme alla normativa.

Nell'ottobre 2018 l'High Court ha ritenuto inammissibile l'azione essenzialmente sulla base di tre rilievi: l'insufficiente prova del danno, l'impossibilità di identificare un interesse comune alla classe rappresentata, l'inadeguatezza dello strumento dell'azione di classe alla luce di una analisi costi-benefici[40]. La Court of Appeal è invece giunta all'opposta conclusione e ha ammesso l'azione di classe, sulla quale pende ora il giudizio di merito, con una pronuncia del 2 ottobre 2019[41]. I punti salienti dell'argomentazione della Court of Appeal sono in sintesi i seguenti:

a) anche in mancanza di danno patrimoniale o danno da ansia e stress, la perdita di controllo sui dati personali dà diritto a un risarcimento in quanto corrisponde per l'individuo alla sottrazione di un bene che ha valore economico;

b) esiste un interesse comune ai componenti della classe, che lamentano la perdita di controllo dei propri dati a causa della stessa condotta asseritamente illecita (dati raccolti senza consenso, nelle stesse circostanze, nello stesso periodo);

c) per quanto onerosa sul piano economico e delle risorse impiegate, l'azione collettiva appare, nel caso di specie, uno strumento idoneo a consentire il ristoro dei soggetti danneggiati laddove venga accertata nel merito la responsabilità del convenuto.

L'intensificarsi delle azioni risarcitorie connesse alla perdita di controllo dei dati mette in luce la questione della possibilità di riconoscere ai dati personali un valore

[40] Lloyd v. Google LLC [2018] EWHC 2599 (QB).
[41] Lloyd v. Google LLC [2019] EWCA Civ 1599.

economico. È una questione, come noto, molto controversa, che sconta l'estrema ampiezza della nozione di dato personale. Va sottolineato che l'idea della patrimonializzazione dei dati personali trova ormai numerose conferme nella normativa europea[42] e, nel nostro ordinamento, ha ricevuto l'avallo del giudice amministrativo[43]. Sarà interessante osservare se anche il giudice civile seguirà la stessa strada e analizzare le implicazioni di eventuali sviluppi della giurisprudenza rispetto a elementi cruciali delle azioni risarcitorie, quali il sistema della prova e le modalità di liquidazione del danno.

5. Conclusioni

Nella moderna economia basata sul digitale, le norme che disciplinano il trattamento dei dati personali si intrecciano in maniera sempre più stretta con quelle relative alla protezione dei consumatori e possono assumere rilievo anche ai fini della verifica di conformità delle condotte d'impresa con le disposizioni a tutela della concorrenza. Per assicurare la certezza giuridica e agevolare la *compliance* da parte delle imprese occorre definire in modo rigoroso gli elementi sostanziali del quadro di riferimento, evitare ingiustificate duplicazioni nell'*enforcement* e nell'irrogazione di sanzioni, chiarire le implicazioni delle violazioni in materia di privacy sul piano delle azioni risarcitorie. È auspicabile uno sforzo congiunto di tutti i soggetti coinvolti e, in particolare, una cooperazione tra le autorità pubbliche incaricate dell'applicazione delle norme[44]. L'obiettivo cui tendere è quello di un ambiente giuridico stabile, trasparente, affidabile che consenta a cittadini e imprese la piena fruizione dei benefici della digitalizzazione nel rispetto dei diritti fondamentali, della libertà di scelta del consumatore e di una sana concorrenza nel mercato.

[42] Cfr. in particolare la Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.
[43] Cfr. Tar Lazio n. 261/2020, cit.
[44] Al riguardo, è apprezzabile l'impegno assunto da Autorità garante della concorrenza, Autorità per le garanzie nelle comunicazioni e Garante per la protezione dei dati personali «a strette forme di collaborazione negli interventi che interessano i mercati digitali, anche attraverso la sottoscrizione di un *memorandum of understanding*»; cfr. Rapporto conclusivo dell'Indagine conoscitiva sui Big Data, cit., p. 121.

Le misure correttive previste dall'art. 58, paragrafo 2, del GDPR, nel sistema sanzionatorio a tutela dei dati personali

DI PAOLO GONNELLI [*]

SOMMARIO: 1. Introduzione. – 2. Il sistema sanzionatorio. –3. Il procedimento per l'adozione delle misure correttive ed i rimedi.

1. Introduzione

Come noto, il sistema normativo attualmente vigente in Italia in materia di protezione dei dati personali è intrinsecamente "asimmetrico", in quanto la quasi totalità delle disposizioni di natura sostanziale è contenuta nel Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (che in prosieguo chiameremo, come tutti, GDPR, acronimo di *General Data Protection Regulation*), mentre una serie di norme "strumentali" e/o integrative , così come tutte le norme di natura sanzionatoria penale sono contenute in quello che resta del nostro "Codice in materia di protezione dei dati personali", originariamente approvato con D.Lgs. 30.6.2003, n. 196, ed ora radicalmente modificato dal D.Lgs. 10.8.2018, n. 101.

Tale "asimmetria", così come il radicale stravolgimento del D.Lgs. 196/2003, deriva dal fatto che quel decreto legislativo costituiva attuazione di una Direttiva europea (la 95/46) e doveva quindi contenere tutta la disciplina organica nazionale attuativa di detta Direttiva, laddove il GDPR, quale Regolamento europeo, è di diretta applicazione nei singoli Paesi membri, così da lasciare legittimo spazio ad una normativa nazionale solo di "attuazione" , ovvero di "integrazione" nei soli casi previsti dalle norme del medesimo GDPR, o comunque nelle materie riservate alla competenza dei singoli Stati, come l'ordinamento giudiziario e le sanzioni penali.

Alla luce di tali principi istituzionali, si sarebbe potuti addivenire ad una sistematica più "pulita" della normativa nazionale, se si fosse abrogato interamente il Codice del 2003 e si fosse emanato al suo posto un nuovo "codice" contenente le solo norme nuove o superstiti. Ma tale soluzione è stata preclusa dalla legge di delega 25 ottobre 2017, n. 163, che poneva fra i principi cui ottemperare nella delega, oltre a quello di abrogare le norme del D.Lgs. 196/2003 incompatibili col GDPR, anche quello di «*modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento*

[*] Avvocato, componente del Consiglio Direttivo dell'AIGE.

(UE) 2016/679 », (fra l'altro con la conseguenza, quasi comica che, per effetto di tale adeguamento, esteso anche al Titolo, il codice italiano è ora formalmente divenuto un Codice nazionale, datato 2003, che reca testualmente «adeguamento dell'ordinamento nazionale» ad un Regolamento europeo del 2016).

Non deve quindi stupire se, soprattutto in tema di misure sanzionatorie penali, occorre leggere la prescrizione sostanziale nel GDPR e la sanzione per l'eventuale inadempimento nel decreto legislativo italiano.

2. Il sistema sanzionatorio

Nel sistema sanzionatorio previsto dalla attuale normativa in materia di protezione dei dati personali occorre ricomprendere tre distinte categorie di strumenti sanzionatori: a) le misure correttive che possono essere adottate dalla Autorità di Controllo (in Italia, "*il Garante"*) ai sensi dell'art. 58, paragrafo 2, del GDPR; b) le misure sanzionatorie pecuniarie, previste dall'art. 83 del medesimo GDPR e disciplinate quanto all'applicazione dall'art. 166 del Codice nazionale; c) ed infine le sanzioni penali, comminate, in coerenza con le previsioni dell'art. 84 del GDPR, dal Capo Secondo del Titolo Terzo del Codice Nazionale («Illeciti penali»: artt. da 167 a 171), nonché da altre norme sparse del medesimo Codice.

Le misure correttive di cui all'art. 58, paragrafo 2, del GDPR rientrano a buon diritto nel concetto di misure sanzionatorie per due ordini di motivi: uno di tipo sistematico ed uno prettamente pratico.

Ed invero, sotto il primo profilo, va considerato che l'art. 83 del GDPR testualmente afferma al secondo comma che «Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) ad h) e j), o in luogo di tali misure»**,** mentre l'articolo 58, paragrafo 2, lettera i), del medesimo GDPR stabilisce testualmente che l'Autorità di controllo ha il potere di «infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso[...]».

Ciò è ben chiaro anche dalla lettura del «considerando» n. 129 del GDPR, nel quale si parla congiuntamente di «poteri correttivi e sanzionatori» attribuiti alle Autorità di controllo, indicandone i criteri di esercizio e la necessaria soggezione a controllo giurisdizionale.

Sotto il profilo pratico, non vi è dubbio che la gran parte delle misure "correttive" previste dal secondo paragrafo dell'art. 58 (si pensi, ad esempio, alla limitazione del trattamento o alla revoca delle certificazioni o all'ordine di sospensione del flusso dei dati verso un paese terzo) ha una notevole portata "afflittiva", non inferiore rispetto a quella delle sanzioni pecuniarie.

E va soggiunto che la inosservanza di una fra le misure correttive in questione costituisce addirittura reato, come si vedrà in appresso.

Veniamo ora all'esame in dettaglio delle misure correttive previste dall'art. 58, paragrafo 2, del GDPR:

Il detto articolo 58, concernente i "poteri" della Autorità di Controllo (che nel nostro sistema nazionale assume, come si è visto, la denominazione di «Garante per la protezione dei dati personali», abbreviata dalla medesima normativa in «Garante») elenca al paragrafo 2 nove categorie di poteri "correttivi", che conviene ricordare espressamente, anche se limiti di tempo non consentono una analisi più dettagliata di ciascuna categoria.

Dispone invero il paragrafo 2 che «Ogni autorità di controllo ha i poteri correttivi seguenti:

a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento;

b) rivolgere ammonimenti al titolare del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;

c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;

d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine;

e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;

f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento

g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;

h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;

i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso*; e

j) ordinare la sospensione dei flussi di dati verso un destinatario di un paese terzo o un'organizzazione internazionale».

La elencazione ora vista è assai più ampia e articolata di quella a suo tempo contenuta nella Direttiva 95/46, che (nell'articolo 28, paragrafo 3, secondo trattino,) si limitava ad attribuire sinteticamente alla autorità di controllo, per quanto qui ci riguarda, «poteri

* Ma questa non è una misura correttiva autonoma, come si è già detto.

effettivi di intervento, come quello di formulare pareri prima dell'avvio di trattamenti […] o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento [...]».

Ed anche la normativa nazionale emanata in attuazione di quella Direttiva, si limitava, nel testo originario dell'art. 154 del D.Lgs. 196/2003, ad attribuire molto sinteticamente al Garante il compito di:

«c) prescrivere anche d'ufficio, ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143;

d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco ai sensi dell'articolo 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali».

Come risulta evidente dalla elencazione contenuta nelle lettere da a) a g) dell'articolo 58, paragrafo 2, del GDPR, la elencazione stessa indica un "principio di gradualità" in forza del quale, a seconda della semplice pericolosità o della gravità dei fatti, si passa dal semplice avvertimento, allo ammonimento, alla ingiunzione di determinati comportamenti, alla limitazione provvisoria o definitiva del trattamento, al divieto dello stesso, e infine all'ordine di rettifica, cancellazione o limitazione del trattamento.

Il principio di gradualità è ulteriormente confermato dalla previsione della possibilità di comminatoria, congiunta o alternativa, di sanzioni amministrative pecuniarie.

Le lettere h) e j) riguardano invece fattispecie particolari di violazioni, entrambe sanzionate molto pesantemente.

Va poi sottolineato che l'inosservanza del provvedimento correttivo di cui alla precitata lettera f) («limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento») è sanzionata, come tale, anche penalmente, ai sensi dell'art. 170 del D.Lgs. 196/2003, a differenza dalla inosservanza degli altri provvedimenti correttivi del Garante previsti dal ripetuto articolo 58, paragrafo 2, del GDPR.

Il legislatore nazionale non si è avvalso della facoltà, accordatagli dal paragrafo 6 dell'articolo 58 del GDPR, di attribuire al Garante ulteriori poteri correttivi, in aggiunta a quelli contenuti nel paragrafo 2 del predetto articolo 58.

3. Il procedimento per l'adozione delle misure correttive ed i rimedi

Il procedimento per l'adozione delle misure correttive previste dall'art. 58, paragrafo 2, del GDPR è disciplinato, congiuntamente a quello per la irrogazione delle sanzioni amministrative pecuniarie di cui all'art. 83 del medesimo GDPR, dal nuovo art. 166 del D.Lgs. 196/2003.

Il procedimento può essere iniziato sia a seguito di reclamo sia a seguito di iniziativa del Garante. L'atto iniziale è costituito dalla notifica al titolare o al responsabile del trattamento della contestazione delle presunte violazioni (salvo che la previa notifica della

contestazione risulti incompatibile con la natura e le finalità del provvedimento da adottare).

Entro trenta giorni dalla notificazione, il presunto contravventore può inviare al Garante scritti difensivi e documenti e può chiedere di essere sentito.

Nella adozione dei provvedimenti sanzionatori, si osservano in quanto applicabili alcune delle norme in materia di sanzioni amministrative contenute nei primi due Capi della legge 24 novembre 1981, n. 689. Va segnalato che non trovano applicazione gli articoli da 10 a 17 e da 29 a 31. In pratica, non trovano applicazione le norme sulla determinazione della misura della sanzione amministrativa né quelle sulla procedura di accertamento e contestazione della violazione, né, infine, quelle sul pagamento in misura ridotta (essendo la procedura di estinzione autonomamente e diversamente disciplinata , come si vedrà in appresso).

È prevista la possibilità di applicazione della pena accessoria della pubblicazione, per intero o per estratto, della ordinanza-ingiunzione che conclude il procedimento sanzionatorio sul sito internet del Garante.

Avverso il provvedimento sanzionatorio del Garante è ammesso, ai sensi dell'art. 78 del GDPR, ricorso giurisdizionale, la cui cognizione è attribuita dall'art. 152 del D.Lgs. 196/2003, alla Autorità Giudiziaria Ordinaria, con il rito di cui all'art. 10 del D.Lgs. 1 settembre 2011, n. 150**,** cioè con il rito del lavoro , con gli adattamenti di cui al citato art. 10.

Entro il termine previsto per il ricorso alla Autorità giudiziaria dal già citato art. 10, comma 3, del D.Lgs. 150/2011 (30 giorni dalla comunicazione del provvedimento, elevati a 60 per i residenti all'estero), il trasgressore e gli obbligati solidali possono, ai sensi del comma ottavo del citato art. 166, «definire la controversia adeguandosi alle prescrizioni del Garante, ove impartite, e mediante il pagamento di un importo pari alla metà della sanzione irrogata».

Il diverso sistema di definizione della controversia, posticipato a dopo la irrogazione della sanzione, anziché anticipato con il pagamento in misura ridotta al momento immediatamente successivo alla contestazione (come prevederebbe l'art. 16 della L. 689/1981, qui non richiamato), è dovuto al fatto che, nel nuovo sistema sanzionatorio in materia di dati personali, disciplinato dall'art. 83 del GDPR, non è previsto un minimo per le sanzioni amministrative pecuniarie, ma solo un massimo, assai elevato (10 o 20 milioni di euro), cosicché sarebbe stato impensabile prevedere il pagamento in misura ridotta pari alla terza parte del massimo della sanzione prevista (secondo il dettato dell'art. 16 L. 689/81, in difetto di previsione di una sanzione minima).

E poiché il legislatore nazionale ha disciplinato congiuntamente la irrogazione delle misure correttive e la irrogazione delle sanzioni pecuniarie, il meccanismo di "definizione" in via amministrativa non poteva che essere differito ad un momento successivo al provvedimento sanzionatorio del Garante, cosicché, a differenza di quanto accade nel sistema generale della legge 689/81, esso non preclude il procedimento sanzionatorio, ma solo il successivo ricorso alla autorità giudiziaria avverso il provvedimento adottato.

Le sanzioni amministrative in materia di protezione dei dati personali: brevi note a margine delle novità introdotte dal Regolamento (UE) 2016/679

DI MARIA BUQUICCHIO [*]

SOMMARIO: 1. Premessa. – 2. Il regime sanzionatorio nel quadro normativo nazionale e comunitario previgente. – 3. Le sanzioni amministrative pecuniarie fissate dal Regolamento (UE) 2016/679 e l'attuazione da parte del legislatore nazionale. – 4. *(segue)* Alcuni spunti di riflessione nella prospettiva interna. – 5. Brevi osservazioni conclusive.

1. Premessa

Le novità introdotte dal Regolamento (UE) 2016/679 (d'ora in avanti, per brevità, il "Regolamento") sul regime sanzionatorio applicabile agli illeciti in materia di protezione dei dati personali hanno attirato l'attenzione di studiosi e operatori del settore sotto una pluralità di aspetti.

Sebbene possa apparire un'utile semplificazione, sarebbe, infatti, riduttivo ritenere che l'unico profilo di rilievo sia quello connesso all'introduzione di un impianto sanzionatorio omogeneo, di diretta attuazione in tutti gli Stati membri.

Accanto alle finalità di armonizzazione, il Regolamento si propone di garantire l'applicazione di «sanzioni pecuniarie […] effettive, proporzionate e dissuasive», fermo restando il rispetto, in ciascuno Stato membro, di «garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta, inclusi l'effettiva tutela giurisdizionale e il giusto processo»[1].

A questo fine il Regolamento ha, per un verso, introdotto specifiche sanzioni pecuniarie, individuate, tuttavia, solo nel limite massimo edittale (peraltro piuttosto elevato), e, per altro verso, ha ampliato il ventaglio di poteri astrattamente esercitabili dalle autorità di controllo designate in ogni singolo Stato membro.

Molti gli aspetti che meriterebbero a tal riguardo un approfondimento, anche tenendo conto, in una prospettiva strettamente nazionale, delle caratteristiche e delle funzioni già assegnate all'Autorità amministrativa indipendente – il Garante per la protezione dei dati personali – a cui questo controllo è rimesso.

L'occasione congressuale impone, tuttavia, di limitare l'analisi a singoli aspetti, ben sapendo che l'argomento si presta a ulteriori e ampi margini di riflessione che per ragioni di sintesi non potranno essere trattati.

---

[*] Avvocato, componente del Consiglio direttivo dell'AIGE. Dottore di ricerca in Diritto Pubblico presso l'Università degli Studi di Roma Tor Vergata.

[1] Cfr. considerando 148 del Regolamento.

In questa prospettiva, si limiterà, quindi, l'analisi che segue alle principali novità introdotte dal Regolamento con riferimento al regime sanzionatorio amministrativo, soffermando poi l'attenzione su alcuni aspetti problematici che sono in realtà comuni alle Autorità indipendenti e che, proprio con riferimento alla materia della protezione dei dati personali, vengono in particolare rilievo.

2. Il regime sanzionatorio nel quadro normativo nazionale e comunitario previgente

Per comprendere sino in fondo l'incisività del cambiamento apportato dal Regolamento sull'intera impalcatura sanzionatoria occorre fare un cenno alla disciplina nazionale e comunitaria antecedente alla sua entrata in vigore.

Il primo tentativo di armonizzazione della tutela del diritto alla protezione dei dati personali a livello europeo si rinviene nell'abrogata direttiva n. 95/46/CE (c.d. direttiva madre) adottata allo scopo «eliminare gli ostacoli alla circolazione dei dati personali» e di garantire un «livello di tutela dei diritti e delle libertà delle persone relativamente al trattamento di tali dati […] equivalente in tutti gli Stati membri» attraverso «un ravvicinamento delle legislazioni»[2].

L'art. 24 della predetta direttiva si limitava, tuttavia, a rimettere agli Stati membri il compito di adottare «le misure [sanzionatorie] appropriate per garantire la piena applicazione delle disposizioni della presente direttiva»[3].

Nell'ambito degli spazi di libertà concessi dalla normativa comunitaria, con la legge 31 dicembre 1996, n. 675 – di recepimento della direttiva n. 95/46/CE – il legislatore nazionale aveva introdotto uno specifico sistema sanzionatorio "a doppio binario", del tutto sbilanciato a favore dell'applicazione di sanzioni penali.

Alle sanzioni amministrative era dedicato un unico articolo (l'art. 39 della l. n. 675/1996) riferito essenzialmente alle ipotesi di omessa esibizione di informazioni o documenti richiesti dall'autorità nell'esercizio della propria attività di controllo o alla

[2] Cfr. considerando 8 della direttiva n. 95/46/CE. Per completezza, occorre precisare che, a livello sovranazionale, il primo atto normativo in materia di protezione dei dati personali risale alla Convenzione del Consiglio d'Europa n. 108 del 1981, ratificata e resa esecutiva con la legge 21 febbraio 1989, n. 98. Scopo della Convenzione è quello di «garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano ("protezione dei dati")» (art. 1). Quanto alle sanzioni, la Convenzione rimette a «Ciascuna Parte» il compito di «stabilire sanzioni e ricorsi appropriati per le violazioni delle disposizioni di diritto interno che danno attuazione ai principi fondamentali per la protezione dei dati» (art. 8).

[3] Lo stesso approccio è stato adottato anche dalla direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche che all'art. 15 co. 2 dispone che «Le disposizioni del capo III della direttiva 95/46/CE relative ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni si applicano relativamente alle disposizioni nazionali adottate in base alla presente direttiva e con riguardo ai diritti individuali risultanti dalla stessa».

violazione delle disposizioni procedurali previste dalla stessa legge per la raccolta dei dati a tutela dei diritti degli interessati[4]. Solo per queste inosservanze il legislatore aveva previsto l'applicazione di sanzioni amministrative, peraltro di modesta entità e con una forbice edittale piuttosto ristretta. Per ogni altra violazione era prevista l'applicazione di sanzioni penali.

Con l'adozione del successivo d.lgs. 30 giugno 2003, n. 196 (c.d. Codice della privacy)[5] l'apparato delle sanzioni amministrative ha ricevuto una più compiuta ed articolata disamina.

Accanto alle sanzioni di natura penale, il legislatore aveva, infatti, introdotto un intero Capo dedicato alle violazioni amministrative (Parte III, Titolo III, Capo I, artt. 161 – 166 d.lgs. n. 196/2003), maggiormente dettagliate nei limiti minimi e massimi allo scopo di adeguare e graduarne l'importo alla gravità delle singole ipotesi di illecito introdotte, a volte molto diversificate fra loro.

Si trattava in ogni caso di sanzioni di modesto importo[6] – tenendo conto, peraltro, delle particolari condizioni economiche dei soggetti cui spesso tali sanzioni erano irrogate[7] – e che, solo dopo le integrazioni apportate dal d.l. 30 dicembre 2008, n. 207, convertito con modificazioni dalla legge 27 febbraio 2009, n. 14[8], potevano raggiungere,

[4] Per un approfondimento sul regime sanzionatorio introdotto dalla l. n. 675/96, *ex multis,* M. MANTOVANI, *Le fattispecie incriminatrici della legge sulla privacy: alcuni spunti di riflessione*, in *Crit. Dir*., 1997, p. 194 ss.; G. CORRIAS LUCENTE, *Commento* sub *artt. 34-38*, in E. GIANNANTONIO, M. G. LOSANO, V. ZENO ZENCOVICH (a cura di), *La tutela dei dati personali, Commentario alla l. 675/96*, Padova, 1997, p. 357 ss. Per una critica al «massiccio uso della sanzione penale» da parte del legislatore nazionale si veda S. SEMINARA, *Appunti in tema di sanzioni penali nella legge sulla privacy*, in *Resp. civ. prev.*, 1998, p. 911 ss.

[5] Il d.lgs. 30 giugno 2003, n. 196 è stato adottato dal Governo allo scopo di riunire e coordinare le norme all'epoca vigenti in materia di protezione dei dati o ad essa connesse (da qui la denominazione convenzionale di "Codice", come si legge nella relazione parlamentare di accompagnamento) e di apportarvi le integrazioni o modificazioni necessarie sia a tale coordinamento, sia «per assicurarne la migliore attuazione» (cfr. art. 1, comma 4, della legge-delega 24 marzo 2001, n. 127).

[6] Solo a titolo esemplificativo, si consideri che per la cessione dei dati per scopi diversi da quelli per i quali erano raccolti o in violazione di altre disposizioni in materia di disciplina del trattamento dei dati personali, l'art. 162, co. 1, d.lgs. n. 196/2003 prevedeva la sanzione amministrativa del pagamento di una somma da cinquemila euro a trentamila euro, poi aumentati da diecimila euro a sessantamila euro dall'art. 44, co. 3, lett. a) del d.l. n. 207/ 2008, convertito con modificazioni dalla legge n.14/ 2009.

[7] Tra le sanzioni di maggior importo inflitte dal Garante per la privacy nella vigenza del precedente quadro sanzionatorio si ricorda l'ordinanza-ingiunzione nei confronti di Google Inc. - 18 dicembre 2013 (Registro dei provvedimenti n. 583) per il servizio Street View e l'ordinanza-ingiunzione nei confronti di Facebook Ireland Ltd e Facebook Italy s.r.l. del 14 giugno 2019 (Registro dei Provvedimenti n. 134) per gli illeciti compiuti nell'ambito del caso "Cambridge Analytica", entrambe dell'importo di 1 milione di euro.

[8] Nella relazione illustrativa al disegno di legge d'iniziativa governativa n. 1305 AS presentato il 7 gennaio 2009 «Conversione in legge del decreto-legge 30 dicembre 2008, n. 207, recante proroga di termini previsti da disposizioni legislative e disposizioni finanziarie urgenti» si legge espressamente che «L'intervento normativo d'urgenza si rende necessario per fronteggiare in maniera efficace gravi fatti criminosi di acquisizione e diffusione illecita di dati personali che si

nei casi più gravi, l'importo massimo di centoventimila[9] o centottantamila[10] euro, eventualmente aumentabile sino al doppio o fino al quadruplo in ragione delle condizioni economiche del contravventore[11].

3. Le sanzioni amministrative pecuniarie fissate dal Regolamento (UE). 2016/679 e l'attuazione da parte del legislatore nazionale

L'evoluzione tecnologica e l'avvertita esigenza di garantire un quadro più solido e coerente in materia di protezione dei dati, che fosse affiancato da efficaci misure di attuazione omogenee in tutti gli Stati membri, hanno indotto il legislatore europeo ad adottare il Regolamento di cui oggi si discute[12]. Ebbene il Regolamento rappresenta un decisivo punto di svolta nel percorso tracciato dalle precedenti direttive, come si avverte sin dai suoi principi ispiratori.

Accanto ai tradizionali principi di trasparenza, non eccedenza e pertinenza del trattamento, il nuovo quadro normativo è, infatti, ispirato a principi del tutto innovativi rispetto alla precedente logica di sistema e volti a rispondere all'esigenza che i dati siano

---

sono verificati specie di recente e provenienti, per lo più, da delicate infrastrutture critiche quali le banche dati di grandi dimensioni e di particolare rilevanza, nonché i connessi fenomeni di "dossieraggio". A tale fine, l'articolo intende introdurre, innanzitutto, specifiche fattispecie aggravate per i suddetti casi, specie quando coinvolgano numerosi interessati o comportino per essi un pregiudizio maggiormente rilevante (comma 7). […] Si prevede un contenuto adeguamento dei limiti minimi e massimi di alcune sanzioni amministrative pecuniarie, specie nei casi di violazioni più gravi, in modo da calibrarne l'efficacia rispetto a situazioni eterogenee, a volte molto diversificate fra loro, che spesso si verificano (commi da 2 a 6 e 10)».

[9] L'art. 162, co. 2 bis, prevedeva, ad esempio, l'applicazione di una sanzione amministrativa da ventimila euro a centoventimila euro in caso di trattamento di dati personali effettuato in violazione delle misure minime di protezione dei dati personali indicate nell'articolo 33 o in caso di trattamento illecito dei dati ai sensi dell'art. 167.

[10] L'art. 162, co. 2 ter, prevedeva che in caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro.

[11] L'art. 164-bis, commi 3 e 4, inserito dall'art. 44, co. 3, lett. c), del d.l. 30 dicembre 2008, n. 207 prevedeva testualmente che «3. In altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, i limiti minimo e massimo delle sanzioni di cui al presente Capo sono applicati in misura pari al doppio. 4. Le sanzioni di cui al presente Capo possono essere aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore».

[12] Significativo in questo senso è il considerando 9 dove il legislatore europeo espressamente riconosce che «la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche». Per un approfondimento, sulle novità introdotte dal Regolamento (UE) 2016/679 e, ancor prima, sul ruolo svolto dalla Corte di Giustizia nella creazione di un diritto alla protezione dei dati personali adeguato all'evoluzione tecnologica, cfr. F. ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679,* in *Eurojus.it,* 5, 2018, p. 18 ss.

tutelati sin dal momento della progettazione e «per impostazione predefinita»[13]. Si definiscono in questo modo i principi di *privacy by default* e *privacy by design*, che trovano una proiezione negli obblighi di "auto-responsabilizzazione" previsti in capo al titolare, responsabile e incaricato del trattamento nella protezione e conservazione del dato personale.

In questo contesto, un ruolo centrale è stato anche assegnato alle autorità di controllo, a cui è attribuito il compito garantire un monitoraggio e un'applicazione coerenti del Regolamento, attraverso l'esercizio di compiti e poteri effettivi, fra cui «poteri di indagine, poteri correttivi e sanzionatori»[14]. Ed è in questa prospettiva che l'art. 58, par. 2 lett. i) del Regolamento conferisce, tra l'altro, all'autorità di controllo (che nel nostro ordinamento si identifica con il Garante per la protezione dei dati personali[15]) il compito di infliggere sanzioni amministrative pecuniarie «effettive, proporzionate e dissuasive» (art. 83, par. 1 del Regolamento).

L'apparato sanzionatorio introdotto, che senz'altro si distingue per la finalità di armonizzazione perseguita, non è stato tuttavia esente da critiche.

Innanzitutto, occorre chiarire che l'impianto si suddivide in base a due categorie generali di violazioni: la prima relativa alla violazione degli obblighi da parte dei soggetti investiti del compito di garantire l'efficace tutela dei dati personali e la seconda relativa, invece, alle violazioni che riguardano i principi base del trattamento dei dati personali[16].

Rispetto ad entrambe le categorie il legislatore comunitario ha individuato le sanzioni amministrative nel solo massimo edittale con soglie particolarmente elevate che arrivano, per la prima categoria, sino a dieci milioni di euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, qualora risulti superiore all'importo predetto; per la seconda categoria di violazioni sino a 20 milioni di euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Importi identici sono previsti anche nell'ipotesi di inosservanza di un ordine da parte dell'autorità di controllo[17].

A questo primo profilo di criticità, connesso all'individuazione degli importi sanzionatori solo nel limite massimo, si aggiunge un ulteriore profilo di indeterminatezza in relazione alla disomogeneità del disvalore delle condotte riconducibili alle due macrocategorie in cui le violazioni sono suddivise: si pensi alla violazione degli obblighi

[13] Cfr. art. 25 del Regolamento.
[14] Cfr. considerando 129 del Regolamento.
[15] Cfr. art. 166, co. 3, d.lgs. 196/2003, come modificato dall'art. 15, co. 1, d.lgs. n. 101/2018
[16] Per un'ampia disamina delle sanzioni amministrative pecuniarie previste dal Regolamento si veda L. BOLOGNINI, C. BISTOLFI, *Le sanzioni*, in E. PELINO, L. BOLOGNINI, C. BISTOLFI (a cura di), *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 685 ss.
[17] Come è stato acutamente osservato, l'art. 83, co. 4 e 5 del Regolamento, «là dove individua quale parametro delle sanzioni amministrative il "fatturato mondiale", vale in effetti a dimostrare la avvertita consapevolezza della posizione economica ora rivestita dagli operatori del mercato», così V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contr. e Impr*., 2018, p. 1098 ss.

imposti al titolare e al responsabile del trattamento o l'omissione della tenuta del registro dei trattamenti, che soggiacciono alla stessa sanzione prevista per la violazione in materia di certificazione, «nonostante nel primo caso la violazione riguardi misure obbligatorie della protezione dei dati, nel secondo un meccanismo soltanto eventuale»[18].

Ulteriori critiche sono state mosse in relazione alla tecnica di costruzione del precetto, «resa assai farraginosa dal rinvio alle norme di disciplina, effettuato in modo tutt'altro che puntuale» in quanto, «anziché richiamare un preciso dovere o divieto sancito dal Regolamento, con indicazione esatta del relativo paragrafo, si effettua un rinvio puro e semplice a interi articoli che, al loro interno, contengono più norme magari rivolte a destinatari diversi»[19].

Tra le critiche mosse, l'argomento di maggior rilievo sembra senz'altro quello connesso all'inasprimento delle sanzioni amministrative pecuniarie individuate dal legislatore solo nel limite massimo, peraltro elevatissimo. Circostanza questa che induce ad osservare come, al di là del *nomen*, le sanzioni amministrative individuate dal legislatore comunitario possano essere giudicate come sanzioni "sostanzialmente penali" alla luce dei noti criteri Engel[20].

Peraltro, in un contesto non privo di criticità, il legislatore delegato, in virtù della facoltà concessagli dall'art. 84 del Regolamento, ha introdotto nel Codice della privacy ulteriori fattispecie cui applicare le sanzioni previste dal Regolamento[21], abdicando, al pari del legislatore europeo, alla prerogativa di graduare il trattamento sanzionatorio. All'autorità competente spetterà, dunque, in ultima istanza il compito di irrogare e graduare le sanzioni amministrative sino al limite massimo edittale previsto dal legislatore europeo[22].

---

[18] In questi termini, L. D'AGOSTINO, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al d.lgs. 10 agosto 2018, n. 101*, in *Arch. Pen*., 2019, p. 21.

[19] L. D'AGOSTINO, *cit.,* p. 21

[20] Tale denominazione risale al *leading case* in cui sono stati affermati, Corte europea dei diritti dell'uomo, Plenaria, 8 giugno 1976, *Engel e altri c. Paesi Bassi*, serie A n. 22, par. 81 e 82, avente ad oggetto sanzioni di carattere detentivo in ambito militare, con cui la Corte ha elaborato alcuni criteri sulla base dei quali è possibile qualificare come sostanzialmente "penali" anche sanzioni di diversa natura, con conseguente applicazione degli istituti e le garanzie tipiche di tutte le sanzioni di carattere punitivo afflittivo. La categoria di sanzioni riconducibili nell'alveo penale si è esteso sino a ricomprendere anche mere afflizioni patrimoniali, tra cui pacificamente rientrano anche le sanzioni amministrative irrogate dalle Autorità amministrative indipendenti.

[21] L'art. 15, co. 1, lett. a) d.lgs. 10 agosto 2018, n. 101 ha sostituito integralmente l'art. 166 del Codice della privacy, introducendo una lunga elencazione di violazioni non direttamente previste dal Regolamento (ad esempio per l'oscuramento dei dati relativi al numero nelle chiamate in entrata) a cui applicare le sanzioni di cui all'art. 83, co. 4 e 5 del Regolamento. Per un approfondimento si rinvia a G. MULAZZANI, *Le sanzioni amministrative in materia di protezione dei dati personali nell'ordinamento europeo ed in quello nazionale*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, p. 791 ss.

[22] Sull'omessa fissazione di un minimo edittale si veda il testo dell'Audizione di Antonello Soro, Presidente del Garante per la protezione dei dati personali, sull'Atto del Governo n. 22 (Adeguamento normativa nazionale circa la protezione delle persone fisiche con riguardo al trattamento dei dati personali) presso Commissioni speciali su atti urgenti del Governo congiunte

A ben vedere, tuttavia, l'approccio adottato dal legislatore nel Regolamento trova la sua giustificazione e, se vogliamo, il suo contemperamento nella dichiarata esigenza che «L'imposizione di sanzioni, comprese le sanzioni amministrative pecuniarie sia assoggettata a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta di Nizza, inclusi l'effettiva tutela giurisdizionale e il giusto processo»[23].

Per altro verso, già il legislatore europeo ha individuato una serie di mitigazioni che circoscrivono l'ampio potere riconosciuto alle autorità di controllo e ne tracciano i confini.

È in quest'ottica che va letto infatti l'art. 83, par. 2, il quale introduce un elenco di criteri che le autorità di controllo devono usare per valutare sia l'opportunità di irrogare una sanzione amministrativa che l'importo stesso della sanzione. Tra questi criteri rilevano, in particolare, la natura, la gravità e la durata della violazione nonché il numero di interessati lesi dal danno e il livello del danno subito; il carattere doloso o colposo della violazione; le misure adottate per attenuare il danno subito dagli interessati; e ancora, eventuali precedenti violazioni commesse; il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso[24].

Proprio l'elenco degli elementi che l'autorità dovrà prendere in considerazione ai fini dell'irrogazione della sanzione dà, peraltro, la misura della centralità del ruolo attribuito dal Regolamento alle autorità di controllo.

Senato e Camera - Ufficio di Presidenza (7 giugno 2018), disponibile al sito www.garanteprivacy.it secondo cui «nella sistematica del Regolamento si delinea un continuum tra provvedimenti inibitori, prescrittivi e monitori da un lato e sanzioni amministrative pecuniarie, dall'altro. Pertanto, la misura minima suscettibile di applicazione a fronte di un illecito è da identificarsi in quelle di cui all'articolo 58, par.2, secondo la gradazione lì indicata, mentre la concreta entità della sanzione amministrativa pecuniaria che si dovesse in concreto irrogare sarà fissata in ragione dei parametri specificamente indicati dall'art. 83, par. 2, Gdpr. In tal senso non vi è alcuna illegittimità costituzionale in quanto la funzione garantista della comminatoria edittale (volta a circoscrivere la discrezionalità dell'organo chiamato ad irrogare la sanzione) resta comunque impregiudicata, dal momento che la scelta del Garante sull'*an* e sul *quantum* della sanzione (dunque anche sulla comminatoria infraedittale) è rigorosamente vincolata dai parametri stringenti di cui all'art. 83, c.2 del Regolamento. […] In ogni caso, la mancata previsione del minimo edittale non determina l'assenza di misure premiali per chi intenda accedere al pagamento in misura ridotta, perché l'art.166, c. 9, consente la definizione della controversia mediante adeguamento alle prescrizioni del Garante e pagamento della metà della sanzione irrogata. Pertanto, l'importo da pagare per estinguere il procedimento è fissato non già con riferimento alla astratta comminatoria edittale ma al quantum concretamente irrogato, consentendo così peraltro un migliore adeguamento della sanzione da applicare in via agevolata alle peculiarità della fattispecie concreta».

[23] Cfr. considerando 148 del Regolamento. Negli stessi termini art. 58 e art. 83, par. 8 del Regolamento.

[24] Per una analisi operativa dei criteri di applicazione delle sanzioni amministrative individuati dall'art. 83, par. 2 del Regolamento, si rinvia a M. IASELLI, *Sanzioni e responsabilità in ambito GDPR*, Milano, 2019, p. 61 ss.

Ulteriore misura di contenimento all'esercizio del potere sanzionatorio si rinviene all'art. 83, par. 3 laddove si chiarisce che, se in relazione allo stesso trattamento o trattamenti collegati il titolare del trattamento o il responsabile viola, con dolo o colpa, varie disposizioni del Regolamento, l'importo totale della sanzione amministrativa pecuniaria non deve superare l'importo specificato per la violazione più grave, così da dirimere anche il verificarsi di un eventuale concorso formale di norme.

Ancora, il considerando 148 del Regolamento introduce la nozione di «violazioni minori» attribuendo all'autorità di controllo il potere di sostituire la sanzione pecuniaria con un ammonimento, ogni qualvolta, all'esito di una valutazione del caso concreto risulti che «la sanzione pecuniaria che dovrebbe essere imposta costituisca un onere sproporzionato per una persona fisica». In termini analoghi al considerando 150 si chiarisce che «Se le sanzioni amministrative sono inflitte a persone che non sono imprese, l'autorità di controllo dovrebbe tenere conto del livello generale di reddito nello Stato membro come pure della situazione economica della persona nel valutare l'importo appropriato della sanzione pecuniaria. Il meccanismo di coerenza può essere utilizzato anche per favorire un'applicazione coerente delle sanzioni amministrative pecuniarie».

A questi strumenti di mitigazione si aggiungono poi le Linee guida elaborate dal Comitato europeo per la protezione dei dati nell'ottobre 2017 che indirizzano le autorità di controllo degli Stati membri nell'interpretazione dei criteri previsti dall'art. 83 del Regolamento «al fine di adottare un approccio coerente all'imposizione di sanzioni amministrative pecuniarie»[25].

Gli strumenti di mitigazione già previsti dal legislatore comunitario e appena illustrati sembrano dunque smentire le critiche mosse all'indeterminatezza dell'apparato sanzionatorio introdotto dal Regolamento.

4. *(segue) Alcuni spunti di riflessione nella prospettiva interna*

Dissolti i dubbi mossi sull'adeguatezza del regime sanzionatorio fissato dal Regolamento, resta, tuttavia, da chiedersi se il procedimento per l'adozione delle sanzioni e l'impianto di tutele giurisdizionali contemplato dall'ordinamento interno sia conforme allo standard previsto dal legislatore europeo e, soprattutto, soddisfi quelle esigenze di effettività e giusto processo a cui il Regolamento in più parti rinvia e che sembrano evocare il necessario rispetto degli obblighi convenzionali richiesti dall'art. 6 della Convenzione europea dei diritti dell'uomo[26] e dal corrispondente art. 47, par. 2, della

[25] Cfr. Linee Guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del Regolamento (UE) n. 2016/679 – WP, adottate il 3 ottobre 2017, disponibili al sito *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.*

[26] Sul rilievo che l'art. 6, par. 1, CEDU assume nei riguardi dei procedimenti amministrativi sanzionatori nazionali, cfr. M. ALLENA, *Art. 6 CEDU. Procedimento e processo amministrativo*, Napoli, 2012.

Carta di Nizza, così riportandoci all'annosa e mai sopita questione sul rispetto di tali garanzie nel nostro ordinamento da parte delle Autorità indipendenti[27].

È, infatti, un dato ormai condiviso alla luce della giurisprudenza della Corte europea dei diritti dell'uomo ("Corte EDU") che il procedimento amministrativo sanzionatorio dinanzi alle Autorità indipendenti non soddisfi le garanzie del «giusto processo» richieste dall'art. 6 della CEDU, e ciò non tanto sotto il profilo dell'indipendenza dell'organo decisorio o del rispetto del contraddittorio, quanto piuttosto sotto il profilo della terzietà.

La stessa Corte Costituzionale ha preso espressamente posizione sull'argomento, in una recente sentenza su una questione di legittimità costituzionale sollevata per la prima volta nella sua storia dall'Autorità Garante della Concorrenza e del Mercato nell'ambito del procedimento sanzionatorio diretto ad accertare un'intesa restrittiva della concorrenza[28]. Disattendendo fermamente il principale argomento utilizzato dall'Autorità per giustificare la propria qualificazione in termini di giudice *a quo*, la Corte Costituzionale ha chiarito che l'Autorità è priva della condizione imprescindibile per poter essere qualificata come organo rimettente, ossia del fondamentale requisito della terzietà.

Due i principali argomenti utilizzati dalla Corte Costituzionale per escludere il requisito di terzietà dell'Autorità Garante.

In primo luogo, è stato evidenziato come, a differenza di altri modelli pure diffusi in altri Stati dell'Unione, nel nostro ordinamento, anche quando funzioni inquirenti e decisorie sono formalmente affidate a due uffici separati, il «raccordo istituzionale» che lega uffici istruttori e organo preposto all'irrogazione della sanzione «in una unità soggettiva indiscutibile» finisce per minarne l'imparzialità nell'adozione del provvedimento sanzionatorio.

Ad ulteriore dimostrazione dell'impossibilità di qualificare l'Autorità come organo giurisdizionale, la Corte costituzionale ha inoltre ricordato come questa partecipi al giudizio di impugnativa di un suo atto, quale sia stato il procedimento che lo ha preceduto, per far valere davanti al giudice lo stesso interesse pubblico di cui è portatrice. Ed è proprio la posizione di parte processuale nei giudizi avverso i propri provvedimenti a determinare una ontologica incompatibilità rispetto alla posizione di giudice terzo e imparziale.

---

[27] La dottrina sull'argomento è assai vasta. Senza pretesa di completezza, cfr. F. CINTIOLI, *Giusto processo, CEDU e sanzioni antitrust*, in *Dir. Proc. Amm*., 2015, p. 507 ss., ai cui riferimenti bibliografici si rinvia. Per una analisi delle pronunce più rilevanti della Corte europea dei diritti dell'uomo sulle garanzie che dovrebbero accompagnare i procedimenti amministrativi al fine di assicurare il rispetto dell'articolo 6 della CEDU, anche nell'ottica di individuare proposte per il rafforzamento delle predette garanzie nei procedimenti dinanzi alle Autorità indipendenti, cfr. ASSONIME, *Diritto all'equo processo e sanzioni delle autorità indipendenti: spunti di riflessione alla luce della giurisprudenza CEDU*, Note e Studi n. 1/2015

[28] Il riferimento è alla sentenza della Corte Costituzionale, 31 gennaio 2019, n. 13. Per un commento alla sentenza cfr. G. GRASSO, *La (pretesa) natura esclusivamente amministrativa delle Autorità amministrative indipendenti chiude la porta del giudizio in via incidentale all'Autorità antitrust. Considerazioni a margine della sentenza n. 13 del 2019 della Corte costituzionale*, in *Giur. cost*., 2019, p. 138 ss.

Si tratta di un argomento già utilizzato dalla Corte di Cassazione proprio con riferimento al Garante per la protezione dei dati personali[29] per confermarne la legittimazione dell'Autorità a partecipare ad un giudizio di opposizione avverso un suo provvedimento. Già in quella circostanza, infatti, la Cassazione aveva chiarito come il Garante per la protezione dei dati personali non potesse essere qualificato come giudice terzo e imparziale.

Chiarita in questi termini la questione, e dunque escluso che nel procedimento sanzionatorio dinanzi al Garante possano dirsi soddisfatte quelle esigenze di effettività della tutela e giusto processo richieste dal Regolamento[30], occorre allora domandarsi se tali tutele siano garantite nella successiva fase processuale, ossia nell'eventuale giudizio promosso avverso il provvedimento sanzionatorio.

D'altro canto la stessa Corte EDU (in particolare nella sentenza *Grande Stevens*[31]) ha chiarito che la Convenzione non preclude che una sanzione (formalmente amministrativa ma sostanzialmente) penale possa essere applicata anche da un'autorità che non presenti le caratteristiche sostanziali del giudice (indipendenza e terzietà); in questo caso, tuttavia, è necessario che il soggetto sanzionato abbia la possibilità di impugnare la sanzione di fronte a un organo giudiziario (terzo, indipendente e imparziale) il quale deve poter esercitare sulla sanzione un sindacato di piena giurisdizione (di "*full jurisdiction"*[32]). In

[29] Cfr. Corte di Cassazione, Sez. I, 20 maggio 2002, n. 7341

[30] Per completezza, si precisa che l'art. 166, co. 9, del Codice della privacy stabilisce che, nel rispetto dell'art. 58, par. 4 del Regolamento, «con proprio regolamento pubblicato nella Gazzetta Ufficiale della Repubblica italiana, il Garante definisce le modalità del procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 3 ed i relativi termini, in conformità ai principi della piena conoscenza degli atti istruttori, del contraddittorio, della verbalizzazione, nonché della distinzione tra funzioni istruttorie e funzioni decisorie rispetto all'irrogazione della sanzione». Il Garante, con Deliberazione del 4 aprile 2019, pubblicata sulla Gazzetta Ufficiale n. 106 del 8 maggio 2019) ha adottato il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, nonché il Regolamento n. 2/2019 concernente l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi presso il Garante per la protezione dei dati personali.

[31] Cfr. Corte europea dei diritti dell'uomo, *Grande Stevens altri c. Italia*, II, 4 marzo 2014 (ric. 18640/10; 18647/10; 18663/10; 18668/10; 18698/10) in *Giorn. dir. amm*. 2014, p. 1053 ss., con nota di M. ALLENA, *Il caso Grande Stevens c. Italia: le sanzioni Consob alla prova dei principi CEDU*. Per un approfondimento sulla sentenza Grande Stevens, anche in relazione alla precedente sentenza *Menarini Diagnostics s.r.l. c. Italia*, II, 27 settembre 2011 (ric. 43509/08) cfr. B. NASCIMBENE, *Autorità amministrative indipendenti e sanzioni "penali". Un'occasione di confronto fra CEDU e diritto UE*, in *Eurojus.it,* 2014

[32] Il concetto di "*full jurisdiction*" è stato elaborato nella giurisprudenza della Corte Edu e definito come la «disponibilità per il cittadino di "un tribunale con giurisdizione sul merito della questione" sia sul fatto come sul diritto, punto su punto, senza mai dover declinare la capacità di conoscere i fatti e di provvedere. In altri termini, come potere del giudice "di riformare qualsiasi punto, in fatto come in diritto, della decisione impugnata resa dall'organo inferiore", e quindi di "esaminare il merito del caso, accertare i fatti e valutare gli elementi di prova" così "da decidere sui diritti della parte interessata"», per questa ricostruzione, nonché per ogni utile riferimento alle sentenze della Corte Edu sull'argomento, si rinvia a F. GOISIS, *La full jurisdiction nel contesto*

particolare «esso deve avere competenza per esaminare tutte le pertinenti questioni di fatto e di diritto che si pongono nella controversia di cui si trova investito»[33] e questo anche laddove vengano in rilievo fatti complessi o valutazioni di carattere tecnico, quali quelle ricondotte in Italia alla discussa nozione di discrezionalità tecnica.

5. Brevi osservazioni conclusive

Se quelle appena menzionate sono le coordinate ermeneutiche attraverso cui valutare l'effettività della tutela giurisdizionale e il giusto processo offerto dal giudice, per i provvedimenti sanzionatori adottati dal Garante della Privacy si potrebbe allora pervenire a conclusioni critiche.

È noto, infatti, che la funzione giurisdizionale in questi casi è sottratta alla giurisdizione del giudice amministrativo e rimessa a quella del giudice ordinario che, non di rado, quel sindacato sulla discrezionalità si esime dallo svolgerlo, limitandosi ad una valutazione di attendibilità. Ne sono un esempio le sentenze adottate dal giudice ordinario sui provvedimenti sanzionatori adottati della Banca d'Italia o dalla Consob, che quasi mai si risolvono in pronunce di annullamento o di riforma.

Ecco allora che alla luce del generale ripensamento del sistema sanzionatorio in materia di protezione dei dati personali quello su cui si dovrebbe riflettere è la tenuta e l'adeguatezza degli strumenti di tutela giurisdizionale offerti dall'ordinamento giuridico interno.

È indiscutibile, infatti, che i poteri del Garante siano cambiati, così come ne è cambiato il ruolo: i provvedimenti sanzionatori non dovranno più mirare solo a punire il trasgressore delle regole con finalità meramente punitive. L'ampiezza dei poteri attribuiti all'Autorità (arricchiti dalla possibilità di adottare misure correttive e di ammonimento in aggiunta o in sostituzione delle sanzioni pecuniarie) dimostra, al contrario, che il fine diretto a cui i provvedimenti sanzionatori aspirano è la cura dell'interesse pubblico collettivo, ossia la tutela dei dati personali.

Alla base della sanzione non vi è più, quindi, il mero interesse all'osservanza delle regole e a punire chi le contravviene, ma l'interesse più ampio alla tutela dei dati.

L'Autorità non si limita più a sanzionare ma attraverso quella sanzione è chiamato a regolare, indirizzando il comportamento dei soggetti sottoposti al controllo ed esercitando dei poteri che compensano – e, forse, giustificano – quei fattori di indeterminatezza che il Regolamento sembra introdurre.

Non è un caso, quindi, che anche i precetti non siano determinati con esattezza e che l'ammontare della sanzione sia rimessa alla sapiente valutazione e all'abilità dell'interprete – qual è appunto il Garante – che in questo nuovo contesto gioca un ruolo fondamentale e assume una centralità assoluta.

---

della giustizia amministrativa: concetto, funzione e nodi irrisolti, in *Dir. Proc. Amm*., 2015, p. 546 ss..

[33] Cfr. Corte europea dei diritti dell'uomo, *Grande Stevens altri c. Italia*, II, 4 marzo 2014, *cit.,* par. 139.

Le ragioni della rinuncia alla definizione di regole puntuali o all'esatta indicazione di limiti edittali sono quindi dettate dal fatto che il potere attribuito all'Autorità non è e non va inteso (solo) nella sua accezione punitiva ma, altresì, come utile strumento di regolazione o più correttamente di amministrazione[34].

Se questi sono quindi i presupposti dell'esercizio del potere sanzionatorio svolto dall'Autorità, per un verso occorrerà valutare, nella giurisprudenza che si andrà formando, l'adeguatezza del sindacato che il giudice ordinario vorrà o potrà svolgere sui provvedimenti sanzionatori adottati dal Garante[35]; per altro verso, l'auspicio o più correttamente la sfida sarà per il Garante quella di costruire una regolazione responsiva attraverso l'adozione di provvedimenti sanzionatori, che siano l'esito di una valutazione accurata, ponderata e motivata, nell'esercizio degli ampi poteri che il Regolamento ha voluto ad essa attribuire.

Questo significa anche che l'Autorità sarà chiamata ad acquisire e rafforzare le proprie competenze tecniche di pari passo con l'evoluzione della tecnologia e con le sfide a cui internet e il web pone di fronte, aprendo la strada ad un dinamismo regolatorio che, a fronte di indubbi vantaggi, richiederà un sapiente contemperamento da parte dell'Autorità con i principi costituzionali di legalità, proporzionalità e personalità della pena.

[34] Sul rapporto strumentale tra sanzione amministrativa e funzione amministrativa non può che rinviarsi al pensiero di A. TESAURO, *Le sanzioni amministrative punitive*, Napoli, 1925, p. 90 ss.

[35] Come di recente chiarito dal Presidente emerito della Corte di Strasburgo Guido Raimondi nella sua *lectio magistralis* in occasione del convegno su «Il controllo di *full jurisdiction* sui provvedimenti amministrativi tra separazione dei poteri e sovranità dell'individuo», Napoli, 9 marzo 2018, «l'estensione e l'adeguatezza del controllo effettuato dal giudice amministrativo [o ordinario] dipende infatti in larghissima parte proprio dai tratti peculiari del caso concreto». Per un approfondimento, nonché per alcuni più ampi riferimenti all'intervento del Presidente Raimondi, si veda L. IANNOTTA, *Considerazioni sul controllo di full jurisdiction sui provvedimenti amministrativi alla luce dell'art. 6 della Convenzione europea dei diritti dell'uomo, vivente nella giurisprudenza della Corte di Strasburgo*, in *Dir. Proc. Amm*., 2019, p. 731 ss.

Protezione dei dati personali: la risposta sanzionatoria all'illecito penale

DI BARBARA CARRARA E ALBERTO ERAMO [*]

1. Il quadro sanzionatorio penale anteriore al Regolamento Europeo; dalla Direttiva al Regolamento.

È tutt'ora ben arduo definire i contorni di un concetto inafferrabile quale può essere quello di privacy, sul quale ormai, a partire dall'originario *right to be alone* coniato da Warren e Brandeis alla fine dell'800[1] sino all'attuale definizione di diritto alla riservatezza nella sua dimensione costituzionalmente riconosciuta, la letteratura giuridica è pressoché sterminata[2]: operazione ancora più difficoltosa ove si tratti, delineato il concetto, di strutturare su di esso un bene giuridico da salvaguardare tramite la sanzione penale.

[*] Avvocati del Foro di Roma.

[1] S.WARREN, L. BRANDEIS, (1890), *The right to privacy*, in *Harvard Law Review*, 4, pp. 193-220.

[2] Sulle definizioni di riservatezza, privacy e diritto alla protezione dei dati personali si rinvia alla oramai amplissima letteratura in argomento, tra i quali si ricorda, in ambito propriamente penale, *ex multis*: F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv.it. dir. proc. pen*., 1967, p. 1079 ss.; F. MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in *Arch. giur*., 1968, p. 61 ss.; V. PATRONO, voce *Privacy vita privata (dir. pen.)*, Enc. dir., vol. XXXV, Milano, 1986, p.574; sui reati in materia di privacy, V. PLANTAMURA, *La tutela penale dei dati personali*, in *Dir. informaz. e informatica*, 2007, 3, 651 ss; A. MANNA, M. DI FLORIO*, Riservatezza e diritto alla privacy: in particolare la responsabilità per omissionem dell'internet provider*, in *Cybercrime* (a cura di CADOPPI A., CANESTRARI S., MANNA A., PAPA M.), Milano, 2019, 892.

Su quel peculiare aspetto positivo e funzionale della privacy[3], che è propriamente il diritto alla protezione dei dati personali[4], l'analisi svolta dalla dottrina penalistica negli ultimi anni è stata ancor più serrata, giacché la concezione stessa di dato personale nella società digitale ha assunto un diverso livello di complessità rispetto alla originaria dimensione prettamente individuale[5]; è stato infatti da più parti evidenziato come il bene oggetto di salvaguardia attraverso la sanzione penale abbia progressivamente perduto il suo carattere esclusivamente individuale per acquisire, invece, una connotazione più marcatamente pubblicistica, in una dimensione interrelazionale in cui primario è l'interesse al controllo di quel particolare patrimonio informativo che sono i dati personali, nonché il loro corretto trattamento[6].

La tutela della riservatezza non trova un riferimento diretto nella Carta costituzionale, ma una costante elaborazione dottrinale e quindi la giurisprudenza ne hanno individuato i presupposti nella salvaguardia dei diritti inviolabili e della personalità dell'individuo di cui all'art. 2 della Costituzione[7] nonché, sul piano sovranazionale, nella Carta dei diritti

[3] Sul dibattito in merito al diverso significato di privacy e riservatezza si veda V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia; elementi per un bilancio ventennale*, in *I dati personali nel diritto europeo* (a cura di CUFFARO V. - D'ORAZIO R. - RICCIUTO V.), 2019, Torino, pp. 3-4.

[4] Espressamente introdotto dall'art.1 del Codice della Privacy, nel cui testo originario si statuiva, al primo comma che *"Chiunque ha diritto alla protezione dei dati personali che lo riguardano*". L'articolo 4, comma 9, della legge 4 marzo 2009, n. 15 aveva poi aggiunto al comma 1 il seguente periodo: *"Le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto ad una funzione pubblica e la relativa valutazione non sono oggetto di protezione della riservatezza personale";* tale ultimo periodo venne poi soppresso dall'art. 14, comma 1, della legge 4 novembre 2010, n. 18. Secondo il testo attualmente in vigore dell'art.1 Codice Privacy "*Il trattamento dei dati personali avviene secondo le norme del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, di seguito «Regolamento», e del presente codice, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona".*

[5] Per una compiuta disamina del fenomeno dei Big Data, nonché delle tecnologie di cloud computing ed al recentissimo fenomeno dell'Internet of things (IOT) si rinvia a D. MESSINA, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Analytica*", in *Federalismi.it*, n.20-2018.

[6] Sul punto, si veda: S. ORLANDO, *I Limiti della tutela penale del trattamento illecito dei dati personali nel mondo digitale*, in *Diritto penale contemporaneo*, 2, 2019, 178-200 che individua una dimensione sociale della privacy già nel concetto stesso di interesse al controllo esterno dei propri dati personali, finalizzato alla giusta utilizzazione dei medesimi; così anche M. LAMANUZZI, che sottolinea la duplice natura del diritto alla protezione dei dati personali come diritto dell'individuo ed interesse della collettività. *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della Privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE*, in *JusOnline*, n.1/2017", 218-265, p. 223; sulla privacy come valore meta-individuale sociale si veda anche A. MANNA, M. DI FLORIO, *Riservatezzza e diritto alla privacy; in particolare, la responsabilità per omissione dell'Internet provider*, in *Cybercrime*, Torino, 2019, 892-941; l'interesse pubblico alla tutela del dato emerge vieppiù ove si consideri che le tipologie delittuose a salvaguardia della riservatezza informatica sono tutte procedibili d'ufficio.

[7] Si veda in tal senso Cass. sez. III, 9 giugno 1998, n. 5658 che identifica la riservatezza in un diritto soggettivo perfetto a tutela di «*situazioni e vicende strettamente personali, ancorché verificatesi fuori dal domicilio domestico, da ingerenze che, sia pure compiute con mezzi leciti e*

fondamentali dell'Unione europea[8], che individua la difesa dei dati personali come diritto autonomo rispetto alla tutela della vita privata e familiare ed al domicilio di cui all'art.7, all'art. 16 par.1 del Trattato sul funzionamento dell'Unione europea[9] e nel diritto al rispetto della vita privata e familiare di cui all'art. 8 CEDU.

Nell'ordinamento giuridico italiano la tutela penale della privacy in ambito penalistico fece invece il suo esordio con la legge 8.04.1974 n. 98 (Tutela della riservatezza e della libertà e segretezza delle comunicazioni), grazie alla quale il codice penale venne integrato con alcune disposizioni specifiche[10].

Occorre rilevare in tal senso come nel codice penale siano presenti diversi reati plurioffensivi attraverso i quali - sia pure in via indiretta - viene tutelato anche il bene privacy, tanto da essere talora definiti reati privacy impropri; un diverso orientamento dottrinale preferisce invece ricomprendere i privacy crimes nell'ambito dei cosiddetti reati propri dello spazio informatico globale, anche noti come reati cibernetici, strutturalmente differenti rispetto a quelli propriamente informatici, caratterizzati dalla previsione esplicita di elementi collegati alle nuove tecnologie.[11]

Nel 1981 venne approvata la legge 121/1981 istitutiva presso il Ministero dell'Interno del Centro elaborazione dati (CED), con la quale venne per la prima volta disciplinata la raccolta dei dati e prevista una sanzione penale qualora, in violazione della legge stessa, vi fosse una indebita comunicazione od un utilizzo comunque non conforme delle informazioni da parte del pubblico ufficiale.

---

senza arrecare danno all'onore, al decoro o alla reputazione, non siano tuttavia giustificate da un interesse pubblico preminente» e per la quale "*la disciplina degli ambiti di tutela della vita privata del soggetto, che seppure non trova espressa menzione nelle disposizioni costituzionali, tuttavia nel complesso dei principi da questa ricavabili (oltre che dal cit. art. 2 anche dall'art. 3, che fa riferimento alla dignità sociale, a parte altri riferimenti che possono trarsi dagli artt. 14, 15, 27, 29 e 41 Cost.) ha il suo primo referente*".

[8] Carta di Nizza, proclamata il 7.12.2000 dal Parlamento europeo, dal Consiglio e dalla Commissione, poi modificata Strasburgo il 12.2.2007; dopo l'entrata in vigore del Trattato di Lisbona ha il medesimo effetto vincolante dei trattati. Articolo 7. *Rispetto della vita privata e della vita familiare.* Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni. Articolo 8. *Protezione dei dati di carattere personale* 1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

[9] Per cui "ogni persona ha diritto alla protezione dei dati di carattere personale che lo riguardano".

[10] Si tratta degli artt. 615 *bis* (Interferenze illecite nella vita privata), 617 *bis* (Installazione di apparecchiature atte ad intercettare o impedire comunicazioni telegrafiche o telefoniche) nonché l'art. 617 *ter* (Falsificazione, alterazione o soppressione di contenuto di comunicazioni o conversazioni telegrafiche o telefoniche).

[11] M. LUBERTO, *I reati informatici contro il diritto alla privacy. La tutela fornita dal D.lgs 196 del 2003 e dal codice penale*, in *Giurisprudenza di merito,* 3, 2008, pp. 898 ss.

Con la legge 31.12.1996 n. 675,[12] venne invece predisposta una prima organica regolamentazione sulla materia, unitamente ad un articolato apparato sanzionatorio a tutela del trattamento dei dati: la scelta legislativa allora si orientò verso una decisa repressione del fenomeno, allargando quindi l'incriminazione al maggior numero possibile di condotte tramite la previsione di fattispecie di pericolo presunto, strutturate attraverso lo schema del reato aggravato dall'evento.

Così, nel capo VIII della L.675/96 vennero espressamente previste ben cinque distinte ipotesi di reato, finalizzate tutte a rafforzare la salvaguardia già predisposta dalla Autorità di controllo sul trattamento dei dati; in particolare, si trattava delle fattispecie di omessa od incompleta notificazione nei casi obbligatoriamente previsti dagli artt. 7 e 28 e dell'art.16 (art.34)[13], del trattamento illecito di dati personali (art. 35)[14][15], della omessa adozione di misure necessarie alla sicurezza dei dati (art. 36)[16], dell'inosservanza dei

[12] La disciplina venne adottata sulla scia delle molteplici sollecitazioni provenienti dall'Europa, a partire dalla Convenzione di Strasburgo del Consiglio d'Europa n.108 del 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati personali" (ratificata in Italia con la L. 21.2.1989 n. 98), nonché dalle diverse Raccomandazioni del Comitato dei Ministri d'Europa, sino alla Direttiva "madre" 95/46/CE del Parlamento Europeo e del Consiglio.

[13] La norma prevedeva un fatto più grave, punito con la reclusione da tre mesi a due anni, nel caso in cui le notificazioni fossero imposte dagli articoli 7 e 28 oppure nelle notificazioni venissero fornite indicazioni inesatte od incomplete mentre nella diversa e più lieve ipotesi della notifica prevista dall'art. 16 comma 1 (omissione delle comunicazioni relative alla cessazione del trattamento dei dati) la pena irrogabile era la reclusione sino ad un anno. Non si mancò di rilevare come, nonostante si trattasse di fattispecie delittuosa, la struttura della norma ricalcasse la contravvenzione di cui l'art. 5 bis L.216/1974 sulla Consob; cfr. G. CORASANITI, *La tutela personale dei dati nella L. 675/1996,* 18.02.1997, in *Interlex - Diritto, Tecnologia, Informazione*, http://www.interlex.it/675/corasan4.htm.

[14] A mente del quale il trattamento di dati personali in violazione di quanto disposto dagli articoli 11, 20 e 27 veniva punito con la reclusione sino a due anni o, qualora il fatto fosse consistito nella comunicazione o diffusione, con la reclusione da tre mesi a due anni; nel secondo comma si sanzionava invece l'ipotesi per cui veniva punito con la reclusione da tre mesi a due anni chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, avesse invece comunicato o diffuso dati personali in violazione di quanto disposto dagli articoli 21, 22, 23 e 24, ovvero del divieto di cui all'articolo 28, comma 3; qualora dal fatto fosse derivato nocumento, la reclusione sarebbe stata da uno a tre anni.

[15] Il testo dell'articolo 35 sull'illecito trattamento dei dati costituirà poi il modello base per tutta la normativa successiva ed infatti secondo la giurisprudenza di legittimità (Cass. pen. 3 n. 28689/2004, Modena; Cass. pen. 5, 28.09.2011 n. 44940) tra l'art. 35 e l'art. 167 del Codice della Privacy del 2003 sussisteva una evidente continuità normativa; ciò nonostante, non si mancò di rilevare come tutta la condotta sanzionabile fosse strutturata sulla violazione di disposizioni della medesima legge, quindi si risolveva di fatto in un delitto di infedeltà od inottemperanza, per cui la fattispecie era di fatto costruita come *clausola sanzionatoria dei precetti extra penali.* Così S. ORLANDO, cit., in *Diritto Penale Contemporaneo*, 2.2019, p.184 che rinvia a P. VENEZIANI, *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali*, in *La tutela penale della persona. Nuove frontiere, difficili equilibri* (a cura di L. FIORAVANTI), Milano, 2001, p. 376.

[16] Per cui chiunque, essendovi tenuto, avesse omesso di adottare le misure necessarie a garantire la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti di cui ai commi 2 e 3 dell'articolo 15, sarebbe stato punito con la reclusione sino ad un anno. Se dal fatto fosse derivato nocumento, la pena era della reclusione da due mesi a due anni, mentre in caso di colpa

provvedimenti del Garante (art. 37)[17], della falsità nelle dichiarazioni e nelle notificazioni al Garante (art. 37 *bis*)[18]; infine, con l'art. 38 veniva irrogata la sanzione accessoria della pubblicazione della sentenza nel caso di condanna per uno dei delitti previsti dalla disciplina in esame, mentre con l'art. 39 si imponevano sanzioni amministrative di carattere pecuniario in caso di omessa comunicazione di informazioni richieste dal Garante oppure in caso di mancata esibizione di documenti.

Suscitò poi un certo interesse la peculiare disposizione di cui all'art. 40 (Comunicazioni al Garante) che prevedeva appunto la trasmissione alla Autorità di controllo - a cura della cancelleria - di copia dei provvedimenti emessi dall'Autorità giudiziaria, in relazione a quanto previsto dalla disciplina generale e dalla legge 23 dicembre 1993, n. 547, in maniera tale da effettuare un adeguato monitoraggio in merito all'applicazione delle sanzioni penali previste nel testo normativo.

L'apparato sanzionatorio così strutturato non incontrò tuttavia il favore unanime della dottrina, ad avviso della quale il ricorso all'incriminazione penale, nell'ambito della riservatezza informatica, avrebbe comunque dovuto essere considerato quale ultima istanza ed unicamente per ipotesi di particolare gravità.[19]

Non si mancò poi di rilevare come, effettivamente, il primario bene di tutela non venisse individuato tanto nella riservatezza, la cui lesione comportava al più un aggravamento di pena, quanto propriamente nella violazione di altre disposizioni, pure contenute nella medesima legge e la cui mera disubbidienza automaticamente veniva sanzionata con lo strumento penale, indipendentemente dal verificarsi di una effettiva offesa al bene protetto.

---

si sarebbe applicata la reclusione fino a un anno; sulla costituzionalità della disposizione per indeterminatezza circa la qualificazione soggetto effettivamente responsabile nonché sulla sproporzionatezza della sanzione si veda G. CORASANITI, *La tutela penale dei dati personali nella legge n.675/96*, in *Interlex - Diritto Tecnologia Informazione*, 18.2.1997.

[17] Secondo il quale chiunque, essendovi tenuto, non avesse osservato il provvedimento adottato dal Garante ai sensi dell'articolo 22, comma 2, o dell'articolo 29, commi 4 e 5 (quindi i provvedimenti attinenti ai diritti di accesso, di certificazione, di cancellazione e di rettifica di cui all'art. 13) sarebbe stato punito con la reclusione da tre mesi a due anni.

[18] Questa disposizione venne inserita tramite l'art.16 del D.Lgs. 28.12.2001 n. 476, recante disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali, a norma dell'art. 1 della legge 21.03.2001 n.127 (G.U. n.13 del 16.01.2002): *Art. 37-bis (Falsità nelle dichiarazioni e nelle notificazioni al Garante). - 1. Chiunque, nelle notificazioni di cui agli articoli 7, 16, comma 1, e 28 o in atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.".*

[19] Si fece riferimento in dottrina a "scelte generaliste e panpenalizzanti", ritenendo peraltro inappropriato il ricorso al modello delittuoso piuttosto che a quello contravvenzionale: così A. MANNA, op.cit., 2001; critico anche S. Seminara, che per parte sua non ritiene appropriata la sanzione penale per "attribuire il massimo rilievo al precetti primari non ancora consolidati e di forzare così il loro impatto sulla società, accelerandone il processo di ricezione": S. SEMINARA, *Appunti in tema di sanzioni penali nella legge sulla privacy*, in *Resp. civ. e prev*, 1998, 4-5, 919.

L'apparato sanzionatorio venne poi ulteriormente rivisto tramite il Decreto Legislativo 28.12.2001 n.467[20], emanato sulla base della legge delega n.127 del 24.03.2001 con cui - a sua volta - venne imposta all'Autorità governativa una generale e ragionata risistemazione della materia tramite l'adozione di un testo unico che coordinasse ed attuasse efficacemente le disposizioni vigenti[21][22]; a tal fine, presso il Dipartimento della Funzione Pubblica fu istituita una Commissione di studio, presieduta dal Prof. Cesare Massimo Bianca[23], che optò per un testo unico di rango legislativo - ritenuto più adeguato sia per il livello del bene giuridico oggetto di tutela e sia per le finalità di consolidamento normativo. Il corpus normativo venne affiancato da un disciplinare tecnico per le c.d. misure minime di sicurezza, che avrebbe eventualmente potuto essere opportunamente adeguato all'evoluzione del settore tramite decreti ministeriali non regolamentari[24].

Così, con l'avvento del Codice in materia di protezione dei dati personali venne abrogata tutta la disciplina legale previgente e la nuova normativa degli illeciti penali nell'ambito del trattamento dei dati personali trovò quindi la sua sede nel Capo II del Titolo III del Codice stesso.

L'obiettivo di fondo della nuova normativa codicistica era l'attuazione del pieno coordinamento sia con le nuove istanze della tecnologia come pure con le indicazioni dell'Unione Europea con riferimento, oltre alla pur fondamentale direttiva Madre, anche alle due successive indicazioni in materia, ovvero alla direttiva 2002/21/CE in materia di comunicazione elettronica e trasmissione telematica di dati e informazioni, nonché alla direttiva 2002/58/CE in tema di trattamento di dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche (meglio nota come direttiva E-privacy[25], poi modificata dalle Dir. 2009/136/CE e 2009/140/CE)[26].

---

[20] Decreto legislativo n.467 del 28.12.2001, Disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali, a norma dell'art.1 della legge n.127 del 24.03.2001.

[21] La legge 675/1996 era stata approvata allo spirare del termine ultimo imposto dall'Europa per il recepimento della direttiva 94/46/CE; per adattare ed integrare la stessa normativa venne approvata - nello stesso giorno - anche la legge 676/96 con cui si delegava l'esecutivo ad implementare opportunamente la disciplina entro 18 mesi (art.2); l'attività di integrazione del sistema complessivo si articolò attraverso nove decreti legislativi e due D.P.R nonché diverse ulteriori specifiche disposizioni, legislative e regolamentari, inserite poi in speciali provvedimenti.

[22] Art. 1, comma 4, legge 24 marzo 2001, n. 127.

[23] La direttiva 2002/58/CE del 12 luglio 2002 impose uno spostamento della scadenza del termine per l'esercizio della delega al 30 giugno 2003 (art. 26 della legge 3 febbraio 2003, n. 14.)

[24] L'allegazione dei codici deontologici e di buona condotta veniva imposto dall'art.20 comma 4 del D.lgs. 467/2001. secondo quanto riportato nella relazione al decreto legislativo le allegazioni non intaccavano minimamente il rango legislativo del testo unico.

[25] In merito alla più estesa nozione di "informazione" adottata dalla Direttiva 2002/58/CE e quindi alla più ampia tutela offerta rispetto alla Direttiva madre, si veda A. MANTELERO, *Si rafforza la tutela dei dati personali; Data Breach notification e limiti alla profilazione mediante cookies*, in *Diritto dell'informazione e dell'Informatica*, XXVIII, Fasc.4-5, 2012, 781-804, p.790.

[26] Il codice si ispirava, secondo la Relazione di accompagnamento, "a*ll'introduzione di nuove garanzie per i cittadini, alla razionalizzazione delle norme esistenti e alla semplificazione".*

Come visto, sin dalle disposizioni generali del nuovo testo venne espressamente introdotto il diritto alla protezione dei dati personali, inteso come diritto fondamentale della persona dotato di autonomia rispetto al più generale diritto alla riservatezza, ed il dichiarato fine del testo unico venne individuato nella generale garanzia a che il trattamento dei dati personali fosse svolto nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Sotto il profilo penalistico, anche se la struttura complessiva dell'apparato sanzionatorio non vide in realtà grandi mutamenti, vi furono tuttavia alcune specifiche modifiche rispetto alle disposizioni previgenti, in cui la prospettiva repressiva - basata sulla anticipazione della tutela - venne parzialmente attenuata, presupponendo piuttosto una salvaguardia integrata, impostata sugli ampi poteri di accertamento e controllo della Autorità del Garante[27], rafforzati nei casi di maggior disvalore dal supporto delle sanzioni penali delineati agli artt. 167-172 del testo codicistico.

I rapporti tra l'Autorità Giudiziaria ed il Garante furono inoltre oggetto di una complessiva revisione[28].

Rimaneva tuttavia di tutta evidenza la predilezione accordata alla sanzione di natura penale anche per violazioni di tipo meramente procedurale, in assoluta controtendenza rispetto ad altri Stati membri dell'Unione[29]; in particolare, nel quadro sanzionatorio, integravano ipotesi di natura penale anche comportamenti volti precipuamente ad ostacolare il corretto funzionamento della Autorità di controllo.

L'apparato sanzionatorio venne differenziato in base alla gravità della condotta; tra le fattispecie delittuose vennero inquadrate le più rilevante ipotesi di cui all'art.167

[27] Le disposizioni di cui agli artt. 161 (Omessa od inidonea informativa all'interessato), 163 (Omessa od incompleta notificazione) e 164 (Omessa informazione od esibizione al Garante) mantennero sanzioni amministrative pecuniarie di assoluto rilievo, la cui applicazione era demandata all'Autorità indipendente.

[28] Secondo Manna, l'Autorità di controllo veniva caratterizzata come il perno del sistema di salvaguardia dei diritti, "*estrinsecando un potere di natura strutturalmente amministrativa e funzionalmente giurisdizionale*" ove anche nell'ambito penale il suo ruolo veniva ulteriormente evidenziato proprio grazie alla collaborazione con l'Autorità giudiziaria: cfr. A. MANNA, cit., p. 37, con riferimento anche all'art. 153 comma 1 lettera g) del Codice, che imponeva al Garante l'obbligo di denuncia per ogni fatto astrattamente configurabile quale reato e perseguibile d'ufficio e del quale fosse venuto a conoscenza a causa od in occasione dell'esercizio delle proprie funzioni; ad avviso dell'Autore però lo stesso obbligo sarebbe comunque stato imposto al Garante dagli art. 361 e 331 del codice penale.

[29] Le motivazioni di una scelta di tal fatta possono ravvisarsi, ad avviso della dottrina, proprio nella diversa natura degli interessi da salvaguardare tramite la disciplina del trattamento dei dati personali, ove questa sia volta a creare un "sottosistema subordinato a regolamentazione amministrativa" in cui gli interessi in questione vengono bilanciati attraverso il ricorso a parametri e procedure predefiniti e la cui tutela viene pertanto anticipata; in tal senso si spiega la scelta penalistica anche per salvaguardare il rispetto delle procedure con cui gli interessi contrapposti vengono determinati. Così A. MANNA, *Prime osservazioni sul Testo Unico in materia di protezione dei dati personali: profili penalistici*, in *Privacy.it*.

(Trattamento illecito di dati) 30 31, art. 168 (Falsità nelle dichiarazioni e notificazioni al Garante)[32] e dell'art. 170 (Inosservanza di provvedimenti del Garante)[33], mentre venne invece adottata la struttura contravvenzionale per l'art. 169 (Misure di sicurezza) [34] e per l'art. 171[35] relativo alla violazione delle disposizioni di cui all'articolo 113 e all'articolo 4, primo e secondo comma, della legge 20 maggio 1970, n. 300.

Tuttavia non si omise altresì di rilevare da voci della dottrina come le perplessità relative alla determinatezza e chiarezza delle singole fattispecie, rilevate in precedenza sotto il vigore della previgente normativa, fossero tutt'altro che superate: la tecnica

[30] Come già rilevato, la disposizione attinente il trattamento illecito dei dati personali nel Codice della Privacy del 2003 presentava il medesimo fatto costituente reato già presente nell'art. 35 della Legge 657/1996; la reale differenza era nel diverso ruolo della lesione al bene protetto che - mentre nell'art 33 veniva configurato come una circostanza aggravante - nell'art 167 divenne condizione obiettiva di punibilità; sotto questo profilo la normativa del '96 veniva ritenuta più favorevole, giacché la circostanza aggravante poteva costituire oggetto del giudizio di bilanciamento.

[31] Art. 167. Trattamento illecito dei dati personali.

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per se' o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per se' o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

[32] Art.168. Falsità nelle dichiarazioni al Garante.

1. Chiunque nelle comunicazioni di cui all'art. 32 bis, commi 1 e 8, nella notificazione di cui all'art. 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara od attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

[33] Art. 170 Inosservanza dei provvedimenti del Garante.

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni.

[34] Art. 169. Misure di sicurezza.

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni.

2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che

[35] Art. 171 (Altre fattispecie).

1. La violazione delle disposizioni di cui all'articolo 113 e all'articolo 4, primo e secondo comma, della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della legge n. 300 del 1970.

legislativa del continuo richiamo a fonti secondarie per la determinazione della condotta punibile, in base allo schema delle norme penali in bianco, presentava indubbi profili di criticità, sia per la loro compatibilità con il principio di riserva di legge e sia con il principio di offensività.

2. Il Regolamento Europeo ed il nuovo quadro sanzionatorio nel sistema italiano di salvaguardia della riservatezza informatica

Con la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea del 4.05.2016 del Regolamento Generale sulla Protezione dei dati (GDPR) n. 2016/679/UE del Parlamento Europeo e del Consiglio del 27.04.2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati e che abroga la direttiva 95/46/CE, nonché della Direttiva (UE) 2016/680 del 27.04.2016[36] - precipuamente attinente alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle Autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati - è stato definito il Pacchetto Protezione Dati e definitivamente superata la Direttiva 95/46/CE, le cui originarie linee operative sono quindi state rivedute e rafforzate tramite le indicazioni della giurisprudenza europea.

Il Regolamento (General Data Protection) è entrato in vigore il 25 maggio 2016[37], con l'espressa previsione dell'obbligo per tutti gli Stati membri di darne piena applicazione entro il 25.05.2018 (art. 99 co. 2), in modo da consentire l'adeguamento dei singoli ordinamenti nazionali entro un termine congruo.

In Italia è stato attuato - secondo quanto previsto dall'art.13[38] della legge 25.10.2017 n.163 (legge di delegazione europea)[39] - attraverso il D.Lgs. 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205).

[36] La direttiva, applicabile a tutti i trattamenti dei dati svolti per finalità istituzionali, sostituisce la Decisione Quadro (2008/977/GAI) che disciplina il trattamento dei dati quando svolto dalle Autorità Giudiziarie e di polizia ed unitamente al GDPR costituisce il cosiddetto "Pacchetto Dati"; in particolare, si veda par. 5.

[37] Il GDPR è stato pubblicato in Italia il 4.07.2016 (G.U.n.50).

[38] L'art. 13 della delega legislativa prevedeva alla lettera e) - quale criterio direttivo specifico nella materia penale - che l'esecutivo provvedesse ad "adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n.196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse".

[39] Legge 25.10.2017 n. 163, Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione Europea, pubblicata in G.U. n.259 del 6.11.2017.

Partendo dal presupposto che il trattamento dei dati personali dovrebbe essere al servizio dell'uomo[40], il fine precipuo del Regolamento è integrare la sicurezza nella protezione dei dati e, nel contempo, agevolare la libera circolazione dei dati nello spazio europeo tramite la semplificazione degli oneri amministrativi e l'uniformità della disciplina fra i singoli Stati membri, così da consentire una tutela di pari forza in ciascuno di essi[41]; in tal senso, ben si comprende la scelta dello strumento regolamentare, le cui disposizioni sono direttamente applicabili senza necessità di intervento legislativo.

La dottrina non ha tuttavia mancato di rilevare le peculiarità del Regolamento in ambito penale, ove si prescrive agli Stati di dare attuazione alle disposizioni entro il 25.05.2018 [42]. Per quanto infatti la competenza delineata in ambito criminale dall'art.83 2^comma TFUE [43]rimanga sempre soltanto accessoria ed indiretta, circoscritta quindi ad

[40] Così, il G.D.P.R. 2016/679 al considerandum n.4: "*Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica*".

[41] Rispetto alla Direttiva madre, il cui obiettivo era la specifica tutela del singolo individuo avverso i titolari del trattamento dei dati personali, il Regolamento - come si vedrà - mira piuttosto a salvaguardare anche l'interesse della collettività, attraverso un severo apparato sanzionatorio diretto a scoraggiare e prevenire le condotte illecite; in questo senso, M. LAMANNUZZI, *Diritto penale e trattamento dei dati personali. I Reati previsti dal Codice della Privacy*, in *JusOnline* n.1/2017, 2018-265, p. 250.

[42] Sul punto, si veda BOLOGNINI, che parla di "quasi direttiva", con riferimento alle sanzioni penali che, secondo il Regolamento, "dovrebbero poter essere stabilite": in L. BOLOGNINI, E. PELINO, C. BISTOLFI C. (a cura di), Il *Regolamento Privacy Europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p.705.

[43] Articolo 83 TFUE (ex articolo 31 del TUE)

1. Il Parlamento europeo e il Consiglio, deliberando mediante direttive secondo la procedura legislativa ordinaria, possono stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni.

Dette sfere di criminalità sono le seguenti: terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata. In funzione dell'evoluzione della criminalità, il Consiglio può adottare una decisione che individua altre sfere di criminalità che rispondono ai criteri di cui al presente paragrafo. Esso delibera all'unanimità previa approvazione del Parlamento europeo.

2. Allorché il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri in materia penale si rivela indispensabile per garantire l'attuazione efficace di una politica dell'Unione in un settore che è stato oggetto di misure di armonizzazione, norme minime relative alla definizione dei reati e delle sanzioni nel settore in questione possono essere stabilite tramite direttive. Tali direttive sono adottate secondo la stessa procedura legislativa ordinaria o speciale utilizzata per l'azione delle misure di armonizzazione in questione, fatto salvo l'articolo 76.

un generico potere di indirizzo, tuttavia, a differenza di quanto a suo tempo statuito con la Direttiva Madre - che per parte sua si limitava alla generica imposizione di "misure appropriate" finalizzate alla piena applicazione delle sue disposizioni nonché alla richiesta di conseguenze sanzionatorie determinate da irrogare in caso di violazione delle disposizioni stesse - il G.D.P.R. contiene invece richiami ben precisi alla materia penale[44], ove solo si osservi che nel Considerandum n.149 si statuisce espressamente che "*Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento. Tuttavia, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di giustizia.*"

La disposizione deve essere letta unitamente all'art. 84 del Regolamento:

1. Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive.

2. Ogni Stato Membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 al più tardi entro il 25 maggio 2018, e comunica senza ritardo ogni successiva modifica.

Quindi, dall'esame congiunto delle due disposizioni, si può concludere come gli Stati Membri vengano esortati ad adottare ("debbano poter stabilire") sanzioni penali effettive, proporzionate e dissuasive sia per le violazioni del Regolamento che per le infrazioni della normativa interna, adottata in attuazione del Regolamento stesso, purchè tali

---

Qualora un membro del Consiglio ritenga che un progetto di direttiva di cui al paragrafo 1 o 2 incida su aspetti fondamentali del proprio ordinamento giuridico penale, può chiedere che il Consiglio europeo sia investito della questione. In tal caso la procedura legislativa ordinaria è sospesa. Previa discussione e in caso di consenso, il Consiglio europeo, entro quattro mesi da tale sospensione, rinvia il progetto al Consiglio, ponendo fine alla sospensione della procedura legislativa ordinaria.

Entro il medesimo termine, in caso di disaccordo, e se almeno nove Stati membri desiderano instaurare una cooperazione rafforzata sulla base del progetto di direttiva in questione, essi ne informano il Parlamento europeo, il Consiglio e la Commissione. In tal caso l'autorizzazione a procedere alla cooperazione rafforzata di cui all'articolo 20, paragrafo 2 del trattato sull'Unione europea e all'articolo 329, paragrafo 1 del presente trattato si considera concessa e si applicano le disposizioni sulla cooperazione rafforzata.

[44] Secondo una diversa dottrina, la riserva di legge sembra in questo caso più una occasione per sollecitare gli ordinamenti nazionali all'uso dello strumento penale: C. CUPELLI C. - F. FICO, *I riflessi penalistici del Regolamento UE 2016/679 e le nuove fattispecie di reato previste nel codice privacy dal d.lgsl 101/2018*, in *I Dati personali nel diritto Europeo*, (a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO), Torino, 2019.

inosservanze non siano già state colpite con le sanzioni amministrative pecuniarie di cui all'art.83.

Giacché le caratteristiche proprie del Regolamento sono la portata generale, l'obbligatorietà integrale e la diretta applicabilità[45], si tratta in questo caso di una situazione del tutto peculiare, ove solo si osservi che il secondo comma dell'art.84 richiede la notifica alla Commissione delle disposizioni sanzionatorie, adottate su sollecitazione del GDPR, entro il 25.05.2018 e che tali prescrizioni potranno autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del Regolamento[46].

Poiché l'Unione dispone in materia penale per l'appunto di un solo potere di indirizzo, non sarebbe quindi stato ravvisabile alcun obbligo di incriminazione in capo agli Stati membri:[47] si rammenti tuttavia come la scelta legislativa sia invece stata preceduta da un ampio ed articolato dibattito in sede di adeguamento della disciplina interna, in merito all'opportunità di abbandonare definitivamente la reazione penalistica e puntare piuttosto sul rafforzamento dell'apparato sanzionatorio amministrativo; è ben significativo il fatto che una delle principali preoccupazioni emerse nel corso dei lavori preparatori della Commissione ministeriale per l'adeguamento della normativa italiana al G.D.P.R. sia stata proprio "lo spettro del bis in idem"[48] e che - sotto questo profilo - il sistema dell'illecito punitivo amministrativo sia apparso senz'altro più consono al trattamento dei dati personali, rispetto invece allo strumento penalistico che, per parte sua, aveva in un certo qual modo deluso molte aspettative[4950].

Il primo orientamento assunto in seno alla Commissione mosse dalla necessaria premessa che il disfavore del Regolamento in merito al doppio binario sanzionatorio appariva del tutto evidente dallo stesso tenore della disposizione di cui all'art. 84[51] - intesa come una norma unicamente residuale rispetto all'art. 83 in tema di sanzioni

[45] Art. 288 TFUE.

[46] Potrà quindi essere utilizzato lo strumento della confisca, anche per equivalente; cfr. C. CUPELLI, R. FICO, cit., p. 1109.

[47] Secondo BOLOGNINI, il legislatore nazionale avrebbe potuto semplicemente applicare le sanzioni amministrative ex art. 83 ed introdurre altre sanzioni pecuniarie ex art.84; di diverso avviso invece LAMANNUZZI, che ritiene invece che non sarebbe stato comunque evitabile un adeguamento dell'ordinamento italiano alle sollecitazioni del Regolamento Europeo: cfr. M. LAMANNUZZI, op. cit., p. 254.

[48] In questo senso, O. POLLICINO, M. BASSINI, *Decreto GDPR, "perchè abbiamo depenalizzato il trattamento illecito dei dati personali",* in *Agenda Digitale*, 17.04.2018.

[49] G. FINOCCHIARO, *Perché abrogare il codice Privacy è la scelta migliore e cosa comporta*, in *Agenda digitale*, 9.04.2018.

[50] Delle perplessità sollevate in merito alla revisione dell'art. 167 Codice Privacy riguardavano anche il fatto che la sua applicazione - eccezion fatta per il noto caso *Google - Vivi Down* - fosse stata in realtà assolutamente limitata; così O. POLLICINO - M. BASSINI, *Perché abbiamo depenalizzato il trattamento illecito dei dati personali*, cit.

[51] Di diverso avviso invece il già visto orientamento di pensiero, per cui invece il G.D.P.R. sembra piuttosto invece sollecitare l'introduzione dai sanzioni differenti ed ulteriori rispetto alle sanzioni amministrative nell'ottica di un doppio binario sanzionatorio; così C. CUPELLI, R. FICO, cit., p. 1108, nonché S. ORLANDO, secondo cui il legislatore delegato si è mosso nella prospettiva di un sistema di tutela integrato multilivello: S. ORLANDO, cit., p. 188.

amministrative pecuniarie - e con cui veniva introdotta la possibilità, per gli Stati Membri, di far ricorso alle "altre sanzioni" purché fossero "effettive, proporzionate e dissuasive" ed applicabili, comunque, per le sole violazioni che non fossero già state colpite in via amministrativa.

Questa lettura avrebbe trovato ulteriore conferma nel considerandum n. 149, ove questo specifica che "l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di Giustizia". Poiché l'interpretazione del principio del *ne bis in idem* in ambito europeo era allora apparsa tutt'altro che rigida e si riteneva che non ci fosse un sistema di coordinamento tra il procedimento sanzionatorio ed amministrativo così efficiente da escludere la duplicazione di sanzioni, prevalse in Commissione la posizione di chi riteneva di maggior prudenza escludere le incriminazioni dal sistema di tutela.

Nonostante queste premesse, l'opzione finale di politica legislativa è stata in realtà alla fine ben diversa: nonostante sia stato adottato un corposo apparato di sanzioni amministrative particolarmente afflittive, nel quadro complessivo di adeguamento delle fattispecie di reato è stato di fatto formalmente depenalizzato il solo art. 169, attinente alle misure minime di sicurezza ed è stata attuata la *abolitio criminis* della fattispecie del trattamento illecito di dati sensibili effettuato senza il consenso dell'interessato per effetto diretto della abrogazione dell'art. 23 Codice Privacy.

Una criticità che si è però immediatamente imposta all'attenzione dei commentatori è derivata, per l'appunto, proprio dalla elevata afflittività delle sanzioni amministrative, nonché dalla loro applicazione congiunta con le pene previste per le condotte delittuose, da cui è ben possibile che derivino situazioni di conflitto sistemiche, anche in considerazione della nozione convenzionalmente penale di sanzione adottata dalla giurisprudenza europea: è noto infatti come i punti di attrito fra l'ordinamento italiano ed il principio del *ne bis in idem* - così come delineato dall'art.4 del protocollo 7[52] allegato alla Convenzione Europea per la salvaguardia dei diritti dell'Uomo, nonché dall'art.50[53] della Carta dei diritti fondamentali dell'Unione Europea - siano sorti in esito alla diversa

[52] Art. 4. (Protocollo n. 7 CEDU- Strasburgo, 22.XI.1984 *Ratificato dall'Italia in forza della L.9.04.1990 n.98)*

Ne bis in idem

1. Nessuno potrà essere perseguito o condannato penalmente dalla giurisdizione dello stesso Stato per un reato per il quale è già stato scagionato o condannato a seguito di una sentenza definitiva conforme alla legge e alla procedura penale di tale Stato.

2. Le disposizioni del paragrafo precedente non impediranno la riapertura del processo, conformemente alla legge e alla procedura penale dello Stato interessato, se fatti sopravvenuti o nuove rivelazioni o un vizio fondamentale nella procedura antecedente sono in grado di inficiare la sentenza intervenuta.

3. Non è autorizzata alcuna deroga al presente articolo ai sensi dell'articolo 15 della Convenzione.

[53] Art. 50 (Carta dei diritti fondamentali UE Nizza, 7.12.2000, Strasburgo,12.12.207)

Diritto di non essere giudicato o punito due volte per lo stesso reato.

Nessuno può essere perseguito o condannato per un reato per il quale è già stato assolto o condannato nell'Unione a seguito di una sentenza penale definitiva conformemente alla legge.

interpretazione fornita dalle Corti in merito ai confini delle definizioni di illecito e di sanzione penale, in forza della quale - in base ad una concezione prettamente sostanzialistica, volta alla tutela del singolo rispetto all'interesse statuale alla soddisfazione della pretesa punitiva - anche una sanzione amministrativa possa di fatto essere considerata al pari di una pena irrogabile per un illecito penale.[54][55]

Attraverso l'applicazione dei noti criteri per la valutazione del livello di afflittività delle sanzioni - delineati sin dal 1976[56] - della qualificazione giuridica dell'illecito nel diritto nazionale, della natura dell'illecito, nonché della natura e del grado di severità della sanzione irrogabile, la CEDU ha infatti ben potuto riconoscere natura sostanzialmente penale a sanzioni formalmente amministrative e quindi individuare una violazione del principio del *ne bis in idem.*

Con la nota sentenza della seconda sezione del 4 marzo 2014, *Grande Stevens e altri c. Italia*, reqq. nn. 18640/10, 18647/10, 18663/10, 18668/10 e 18698/10, la Corte è tornata sul maggior peso da attribuire ai criteri del fine dell'illecito ed alla severità della sanzione rispetto alla qualificazione giuridica fornita dall'ordinamento nazionale; criteri questi da applicare in via alternativa o cumulativa ove «l'analisi separata di ogni criterio non permetta di arrivare a una conclusione chiara», essendo sufficiente che «il reato in causa sia di natura "penale" rispetto alla Convenzione, o abbia esposto l'interessato a una sanzione che, per natura e livello di gravità, rientri in linea generale nell'ambito della "materia penale"».

In merito poi al criterio attinente alla severità della sanzione *irrogabile* in base alla disposizione normativa, la Corte non ha mancato di sottolineare come elevati livelli punitivi siano sintomatici della natura repressivo - punitiva del sistema delle sanzioni che - al di là della qualificazione attribuita dall'ordinamento interno - è propria di una funzione dissuasiva tipicamente penalistica. Anche in merito alla sostanza del fatto contestato, Strasburgo riprese la nozione sostanziale di i*dem factum,* già adottata nella pronuncia Zolotukhin vs. Russia (Grande Chambre 10.02.2009), per richiedere un accertamento specifico sulla unicità del fatto per il quale si sia proceduto alla duplicazione dei giudizi.

---

[54] Sul divieto di bis in idem, *ex multis,* si veda: B. NASCIMBENE, *Ne bis in idem, diritto internazionale e diritto europeo*, in *Diritto Penale Contemporaneo*, 2.5.2018; P. COSTANZO P., L. TRUCCO, *Il principio del ne bis in idem nello spazio giuridico nazionale ed europeo, in Consulta online*, 2015, Fasc. III; A. PROCACCINO, *Oltre la matière pénale. I bis in idem tra procedimento penale e procedimenti disciplinari*, in *Diritto pubblico comparato ed europeo*, Fasc. IV, ott.-dic.2019, 1073-1112; M. OROFINO, *Ne bis in idem e sistema sanzionatorio nella disciplina della protezione dei dati personali dopo l'adozione del GDPR,* in *Diritto pubblico comparato ed europeo*, Fasc. IV, ott.- dic. 2019, 1139-1174;

[55] Sul dialogo fra le Corti in materia si veda F. BAILO, Il *bis in idem e la difficile definizione della nozione di sanzione tra Corte Edu, CGUE e Corte Costituzionale*, in *Diritto pubblico comparato ed europeo*, Fasc. IV, ott-dic. 2019, 1221-1238

[56] Nella nota decisione della Corte Edu, sent. 8 giugno 1976, *Engel e a. c. Paesi Bassi,* da cui la definizione di Engel criteria poi comunemente in uso; a far data da questa pronuncia e sulla base della successiva evoluzione giurisprudenziale, la Corte di Strasburgo ha adottato un proprio criterio sostanziale su quel che deve essere considerato reato ai fini della applicazione delle garanzie convenzionali.

Nel caso specifico la Corte in sostanza denunciò l'incompatibilità con i diritti umani salvaguardati dalla CEDU con il sistema di doppio binario amministrativo - penale su cui era strutturato il sistema repressivo dei *market abuse*; al di là tuttavia del caso concreto, il decisum mise seriamente in discussione la possibile coesistenza con il sistema convenzionale di tutti quei settori degli ordinamenti nazionali in cui il sistema di tutela fosse organizzato su un doppio binario parallelo che, potenzialmente, avrebbe potuto predisporre le condizioni per una violazione del diritto al *ne bis in idem* che fosse connaturata al sistema stesso.

La censura mossa dalla Corte si basò pertanto sulla qualificazione sostanzialmente penale sia della procedura amministrativa quanto delle sanzioni alla medesima correlate e, conseguentemente, con l'applicazione delle guarentigie previste dal sistema convenzionale, tra cui appunto il divieto di duplicazione di giudizi per il medesimo fatto[57].

La posizione della Corte venne poi parzialmente modificata nella pronuncia del 15.11.2016 (Grande Chambre) A e B c. Norvegia (ric. n. 24130/11 e 29758/11) ove - fermi restando i criteri Engel - si è aperta invece una possibilità al doppio binario sanzionatorio. La Grande Camera ha infatti affermato che non viola il *ne bis in idem* convenzionale l'esistenza di un giudizio penale pendente nei confronti di chi sia già stato sanzionato in via definitiva sul piano amministrativo, purché *sussista tra i due procedimenti una connessione sostanziale e temporale sufficientemente ristretta*.[58]

Per quanto attiene invece la posizione assunta dalla Corte di Giustizia della Comunità Europea, nel caso Bonda (Corte di Giustizia, Grande sez., sent. 5 giugno 2012, *Bonda*, C-489/10, § 37) a Lussemburgo vennero rielaborati gli Engel criteria adottando un metodo casistico ma rinviando comunque alle corti nazionali per la verifica in merito alla loro sussistenza nel caso concreto; anche nella altrettanto nota sentenza Fransson (CGUE, Grande sez. C-617/10, 26.02.2013, Aklagaren contro Hans Akerberg Fransson) la Corte ha specificato che l'art. 50 della Carta di Nizza non impedisce, di per sè, che uno Stato membro imponga, per le medesime violazioni di obblighi dichiarativi in materia di IVA, una combinazione di sovrattasse e sanzioni penali, giacchè è conferita allo Stato membro la libertà di sanzionare le condotte sia con l'inflizione di sanzioni amministrative che penali oppure con una combinazione delle due, "*al fine di assicurare la riscossione di tutte le entrate provenienti dall'IVA e tutelare in tal modo gli interessi finanziari*

57 F. VIGANÒ, *Ne bis in idem e contrasto agli abusi di mercato: una sfida per il legislatore e i giudici italiani*, in *Diritto penale contemporaneo*, 2016, I, 186 ss.; F. VIGANÒ, *Doppio binario sanzionatorio e ne bis in idem: verso una diretta applicazione dell'art.50 della Carta? (A margine della sentenza Grande Stevens della Corte EDU), ibidem*, 2014 3-4, 219-238.; A.F. TRIPODI, *Uno più uno (a Strasburgo) fa due. L'Italia condannata per violazione del ne bis in idem in tema di manipolazione del mercato*, in *Diritto Penale Contemporaneo*, 9 marzo 2014.

[58] In merito, F. VIGANÒ, *La Grande Camera della Corte di Strasburgo su ne bis in idem e doppio binario sanzionatorio*, "Diritto Penale Contemporaneo, 18.11.2016; L. DEAGLIO, *Il compendio sanzionatorio della privacy sotto la lente del ne bis in idem sovranazionale e della Costituzione*, in *Diritto penale contemporaneo*, 2-2019, 201-210.

dell'Unione", spettando sempre al giudice del rinvio la valutazione, sulla base dei criteri Engel - Bonda, circa la ammissibilità del cumulo sanzionatorio.

Ciò nonostante, all'indomani del già visto nuovo indirizzo interpretativo assunto dalla Corte di Strasburgo con la decisione A e B contro Norvegia, anche la CGUE ha ripreso il criterio della "*sufficiently close connection in substance and time*" nel caso Menci (CGUE, Grande sez., 20.03.2018, Menci, C-524/15; si vedano anche i paralleli Garlsson Real Estate e a. C-596/16; Di Puma e Zecca C-596/16 e C-597-16)[59] per cui devono essere differenti gli scopi perseguiti dai procedimenti e si devono prevedere meccanismi di coordinamento per contenere gli oneri della ricerca e dell'accertamento della prova, la doppia risposta punitiva deve essere prevedibile e il principio di proporzionalità deve essere rispettato dal cumulo sanzionatorio; i procedimenti devono avere un collegamento cronologico e gli illeciti devono colpire profili complementari della stessa condotta.

Non è la prima volta che l'Europa rinvia alla scelta dei singoli stati in merito al mantenimento di un sistema a doppio binario rispetto al medesimo fatto, che presenta il vantaggio di una sanzione amministrativa comminata con immediatezza in esito ad un procedimento poco formalizzato e poco garantito e, nel contempo, di una sanzione penale più incisiva sotto il profilo della deterrenza. Il diritto eurounitario, nel contempo, raccomanda il rispetto del diritto convenzionale al *ne bis in idem* che - secondo il disposto dell'art. 6 TUE - è anche principio del diritto dell'Unione stessa[60].

Tuttavia, ad avviso di una corrente dottrinale, i criteri elaborati dalle Corti sovranazionali non consentiranno di escludere il pericolo del *ne bis in idem* nella disciplina privacy recentemente introdotta. L'afflittività delle misure amministrative sembra infatti rinviare espressamente ad una finalità deterrente e retributiva propria della sanzione penale[61], motivo per cui non sembra rispettato il parametro imposto dalla giurisprudenza sovranazionale sulle diverse finalità che dovrebbero perseguire gli apparati sanzionatori per escludere il bis in idem. Anche il criterio del coordinamento dei procedimenti non appare soddisfatto, stante il meccanismo di coordinamento tra le Procure e l'Autorità di controllo (art. 167 commi 4 e 5) che non appare tale da poter escludere la duplicazione di giudizio[62].

---

[59] F. BAILO, *Il* bis in idem *e la difficile definizione della nozione di sanzione tra Corte Edu CGUE e Corte Costituzionale*, in *Diritto pubblico comparato ed europeo*, Fasc. 4, ottobre - dicembre 2019, 1221-1238, cit.

[60] F. VIGANÒ, *Ne bis in idem e contrasto agli abusi di mercato: una sfida per il legislatore e i giudici italiani*, cit.186 ss.; F. VIGANÒ, *Doppio binario sanzionatorio e ne bis in idem: verso una diretta applicazione dell'art.50 della Carta? (A margine della sentenza Grande Stevens della Corte EDU), ibidem*, 2014 3-4, 219-238.

[61] Così L. DEAGLIO, *Il Compendio sanzionatorio della nuova disciplina della privacy sotto la lente del ne bis in idem sovranazionale e della Costituzione*, in *Diritto Penale Contemporaneo*, 2-2019, 201- 212, p. 208.

[62] Si rileva infatti come la collaborazione tra il Garante e le Procure non appaia bilanciata e biunivoca giacché, a fronte della laconicità della norma sugli obblighi di informativa imposti alla Procura (art. 167 c.4), ben più complessi ed articolati sembrano essere gli adempimenti imposti al Garante dal comma 5 del medesimo articolo, oltre la fatto che nulla viene chiarito in merito

Non si può che concordare con la stessa dottrina, ove solleva le medesime perplessità sul criterio della proporzionalità della pena, poiché l'art. 167, 6° comma prevede una circostanza attenuante ad effetto comune, con una diminuzione di pena applicabile sia allo stesso 167 che al 167 *bis* (diffusione dati) che al 167 *ter* (fraudolenta acquisizione): "*quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa"*: la disposizione presuppone quindi una applicazione congiunta delle sanzioni, ma il riferimento è solo alla sanzione pecuniaria irrogata e riscossa, senza alcun riferimento all'ipotesi in cui il procedimento penale finisca prima di quello amministrativo. Per l'applicazione della attenuante si richiede inoltre la avvenuta riscossione della sanzione, elemento questo che pone seriamente in dubbio l'effettività del coordinamento richiesto per la doppia risposta punitiva.

La profonda revisione dell'apparato sanzionatorio penalistico nel codice della privacy è stata predisposta - sulle indicazioni della legge di delegazione europea (all'articolo 13 comma 3)[63] - con l'intento di abrogare espressamente le disposizioni del Codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel Regolamento (UE) 2016/679 ed adeguare il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del Regolamento con previsione di "sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse" ed evitare quindi il *bis in idem,* attraverso una riformulazione oppure una opportuna depenalizzazione delle fattispecie previste dal GDPR come violazioni amministrative[64]: l'opzione legislativa, tuttavia, si è limitata ad una complessiva opera di risistemazione.

Il problema si è posto in tutta evidenza quindi per quei fatti che possono assumere rilievo penale secondo il sistema sanzionatorio disegnato dal decreto attuativo ma che verranno a loro volta qualificati anche come illeciti amministrativi: il riferimento è quindi alle violazioni in tema di servizi di comunicazioni elettronica, nonché alle violazioni di cui all'art. 2 *sexies*, concernenti il trattamento, per motivi di interesse pubblico rilevante, di categorie particolari di dati personali, alle violazioni previste dall'art. 2 septies relative

alla sorte del procedimento amministrativo dopo la trasmissione degli atti alla Procura da parte della Autorità di controllo; così L. DEAGLIO, cit., p. 205.

[63] Ad avviso di D'AGOSTINO, tuttavia, l'ampiezza della delega ha dato adito a più di una perplessità - con riferimento all'art.76 Cost. - per mancanza di opportuni principi e criteri direttivi in relazione alla riforma dell'apparato sanzionatorio penale, soprattutto ove si confronti la delega in merito al sistema sanzionatorio amministrativo; in questo caso i principi ed i criteri direttivi vengono recuperati attraverso il richiamo al Regolamento che - a differenza di quanto accade per il settore penale - fornisce ogni indicazione di dettaglio; né, ad avviso di questo Autore, sembra si possa rinvenire alcun criterio direttivo generale da aggiungere alla legge di delegazione neppure nell'art. 32 L.234/2012, per cui il legislatore delegato non avrebbe potuto introdurre le nuove fattispecie di cui all'art 167 bis e 167 ter come pure non avrebbe avuto neppure la possibilità di rivedere l'apparato sanzionatorio penale preesistente; L. D'AGOSTINO, *Commento al D,Lgs 10.08.2018 n.101*, in *Archivio penale* n.1-2019, p. 26.

[64] Sulla opportunità di depenalizzare le fattispecie di pericolo astratto dirette alla tutela di funzioni si veda V. MANES - F. MAZZACUVA, cit., p. 177.

le misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute oppure alle violazioni di cui all'art 2 *opties* nell'ambito del trattamento dei dati relativi a condanne penali, misure di sicurezza e reati.

È stata intravista una possibile soluzione al problema tramite ricorso al principio di specialità di cui all'articolo 9 della legge 689/1981[6566] a mente del quale, quando il medesimo fatto è punito da una disposizione penale e da una disposizione che prevede una sanzione amministrativa, ovvero da una pluralità di disposizioni che prevedono sanzioni amministrative, si applica la disposizione speciale: ove, nel caso, il riferimento sarebbe agli elementi specializzanti di cui al sistema di tutela del trattamento illecito dei dati configurato dagli artt. 167, 167 *bis* e *ter* Codice Privacy, alla quale sembra tuttavia essere di impedimento sia la peculiare tipologia delle sanzioni privacy quanto la già vista disposizione di cui all'art. 167 comma 6, che sembra presumere il concorso tra illeciti amministrativi e penali.

3. Le novità

3.1. Il trattamento illecito di dati personali di cui al rinnovato art 167 Codice Privacy

La disposizione legislativa oggetto di maggiori discussioni, all'indomani della pubblicazione del decreto di adeguamento al G.D.P.R., è sicuramente la fattispecie relativa al trattamento illecito di dati di cui all'art.167.

La norma è stata completamente rivisitata[67] per adeguarla opportunamente alle nuove tecnologie ed è precipuamente finalizzata ad una miglior salvaguardia di quello che la dottrina oramai non esita più a definire quale il vero e proprio sistema - privacy .

«Art. 167 (Trattamento illecito di dati). - 1. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, e' punito con la reclusione da sei mesi a un anno e sei mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.

[65] Su cui E. PENCO, *Il principio di specialità amministrativa*, in *Diritto penale contemporaneo*, 3, 2015, 63-70.
[66] Così V. MANES, F. MAZZACUVA, cit. p.177; si veda anche C. CUPELLI, R. FICO, cit., p. 1110.
[67] L'art. 15 comma 1 lettera b) del D.Lgs 101/2018 ha completamente sostituito il testo previgente dell'art. 167.

3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.

4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.

5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.

6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.»;

Si tratta, come è evidente, di fattispecie di assoluto rilievo nel sistema complessivo delineato dal Legislatore, nel quale - rispetto all'apparato normativo preesistente - è stata di fatto abrogata la sola disposizione dell'art. 169 (attinente le misure minime di sicurezza).

Sono state invece inserite inedite ipotesi di reato sia tramite le fattispecie di nuova formulazione previste dagli art. 167 *bis* e 167 *ter* sia tramite la novellazione del secondo comma dello stesso art. 167, relativo al trasferimento dei dati personali all'estero.

Nella nuova formulazione del primo comma dell'articolo 167 risalta evidente l'assenza del riferimento alla condotta di trattamento dei dati come in realtà a qualsiasi altra tipologia operativa[68]; l'azione delittuosa viene così identificata nella violazione delle disposizioni attinenti i dati relativi al traffico (art. 123), i dati relativi all'ubicazione diversi dai dati relativi al traffico riferiti agli utenti o agli abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico (art.126), alle comunicazioni indesiderate tramite l'uso di sistemi automatizzati di chiamata o di comunicazione elettroniche di chiamata (art. 130) o nel caso di violazione del provvedimento del Garante di cui all'art. 129, relativo alle modalità di inserimento e di successivo utilizzo dei dati personali relativi ai contraenti negli elenchi cartacei od elettronici a disposizione del pubblico; si tratta di ipotesi tutte attinenti ai dati personali, per le quali viene prevista una sanzione della reclusione da sei mesi ad un anno e sei mesi, mentre sono venuti meno i riferimenti agli abrogati articoli 18, 19 e 20, relativi alle regole per i soggetti pubblici.

[68] Il precetto viene quindi descritto come violazione di una norma extrapenale, senza alcun riferimento ad una condotta commissiva; tuttavia, nel secondo comma rientra il riferimento specifico alla condotta attiva del trattamento dei dati personali, di cui peraltro rimane inalterato il riferimento nella rubrica.

È venuto meno anche il richiamo all'abrogato art. 23 sul trattamento effettuato senza il consenso degli interessati, al momento oggetto della sola sanzione amministrativa di cui all'art. 83 par. 5 lettera a)[69].

Il secondo comma si riferisce invece propriamente al più delicato settore dei dati sensibili e giudiziari ed in questo caso la condotta delittuosa consiste nel trattamento di dati personali di cui agli art. 9 (Trattamento di categorie particolari di dati personali) e 10 (Trattamento dei dati personali relativi a condanne penali e reati) del G.D.P.R., quando effettuato in violazione degli articoli 2 *sexies* (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante) e 2 *octies* (Principi relativi al trattamento di dati relativi a condanne penali e reati), dell'art. 2 *septies* (Misure di garanzie per il trattamento dei dati genetici, biometrici e relativi alla salute), oppure nella mancata adozione delle misure ed accorgimenti a garanzia dell'interessato che l'Autorità indipendente può prescrivere in caso di trattamenti svolti per l'esecuzione di un compito di interesse pubblico ai sensi dell'art. 2 *quinquiesdecies* del Codice.

La sanzione prevista per ciascuna di queste violazioni è la reclusione da uno a tre anni.

La medesima sanzione è prevista anche nel terzo comma, ove viene introdotta la fattispecie del tutto nuova relativa al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento ed in cui viene prevista la possibilità del trasferimento di tali dati, esclusivamente attraverso una articolata procedura diretta a verificare l'adeguatezza del livello di protezione predisposto nel paese di destinazione.

Gli ultimi tre commi dell'articolo sono dedicati alla definizione dei rapporti tra il Garante e l'Autorità Giudiziaria: viene in essi previsto un sistema di comunicazioni tra la Procura e l'Autorità di controllo, sul quale ci si è già soffermati e che presenta alcuni elementi oscuri, poiché a fronte della laconicità del quarto comma - che si limita a prescrivere un generico obbligo di informativa a carico del Pubblico Ministero allorché abbia notizia dei soli reati previsti nei primi tre commi della medesima disposizione - ben più articolata appare invece l'attività richiesta al Garante che, qualora rilevi qualsiasi ipotesi di reato attinente alla riservatezza, dovrà inviare tutta la documentazione all'Autorità giudiziaria, corredata da una relazione illustrativa.

Si noti al proposito che, mentre non vi è indicazione alcuna circa il termine per la comunicazione disposta dal PM, il Garante dovrà invece necessariamente provvedere al proprio incombente prima della fine delle sue attività accertative.

[69] Si condivide pienamente l'opinione di chi ritiene vi sia stata una parziale *abolitio criminis* e quindi, una continuità solo per le ipotesi superstiti; così L. D'AGOSTINO, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101,* in *Archivio Penale,*1, 2019, pp 1-58: 31. Sulla questione della assenza del consenso quale elemento essenziale della fattispecie si veda anche S. ORLANDO, op. cit., p. 189, secondo il quale l'abrogazione parziale della norma sulla parte attinente al consenso - unitamente al disvalore incentrato sul nocumento - ben rispondono alla finalità di restringere ulteriormente l'area del penalmente rilevante.

Nel sesto comma viene introdotta infine una novità di assoluto rilievo nell'ambito del complessivo sistema e consistente in una specifica attenuante nel caso sia stata già applicata e riscossa la sanzione pecuniaria da parte del Garante e si proceda comunque per la fattispecie delittuosa[70].

Da una complessiva lettura della disposizione non appare superata la criticità - già segnalata in dottrina a proposito del testo previgente - relativa alla tecnica di redazione delle fattispecie di reato basate sul sistema della norma penale in bianco - e quindi sul rinvio *tout court* ad altri precetti che, a loro volta, richiamano fonti ulteriori[71] - rendendo così estremamente difficoltosa la ricostruzione e la identificazione della fattispecie astratta, con evidenti problemi di determinatezza e chiarezza ermeneutica.

La norma presenta in apertura una clausola di riserva (salvo che il fatto costituisca più grave reato) posta a ribadire la natura sussidiaria della fattispecie[72]; si tratta di reato comune ("chiunque") che non richiede pertanto peculiari qualità nel soggetto agente[73].

Sul versante dell'elemento soggettivo, la norma richiede espressamente il dolo specifico alternativo di danno o di profitto ("al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato"), sebbene il primo schema di decreto legislativo avesse inizialmente escluso la finalità di "recare ad altri danno", proprio in relazione al diverso ruolo del nocumento quale elemento della fattispecie (aspetto sul quale ci si soffermerà più diffusamente nel prosieguo).

Non va tuttavia omesso di ricordare che sul punto era intervenuto lo stesso Garante, che aveva invitato a considerare il nocumento "*in ragione dell'esigenza di presidiare con la sanzione penale condotte connotate da un simile disvalore, anche quando sorrette dal dolo di danno e non solo da quello di profitto. Tale modifica consentirebbe inoltre di assicurare una maggiore continuità normativa con la fattispecie vigente e di evitare gli effetti (anche sui processi in corso) dell'abolitio criminis che si dovesse ravvisare, in parte qua, per effetto della novellazione proposta*»[74].

---

[70] Un orientamento dottrinale ravvisa in questo mini-sistema il "salvacondotto" per il mantenimento delle fattispecie penali a fronte delle ventilate ipotesi di depenalizzazione pure avanzate in sede di adeguamento della disciplina interna al Regolamento, giacché proprio le disposizioni di coordinamento tra Procure e Garante assurgerebbero a correttivi di salvaguardia per evitare il pericolo di violazioni del principio di nel bis in idem ribadito dal considerandum n.149 del GDPR. In tal senso, G. DE BERNARDO, *Le sanzioni penali nel nuovo D.Lgs.n.101/2018, in* "Giurisprudenza penale web", 2019, 2, pp. 1-7:4; ma si veda anche il par. 2 di questo contributo.

[71] Per cui, in relazione alla precedente disciplina, si giunse a parlare di "vertigine combinatoria"; così G. CORRIAS LUCENTE, *Profili penali della recente legge sul trattamento dei dati personali*, in *Studium Juris*, 1998; con riferimento al "gioco dell'oca normativo" si veda anche P. TRONCONE, *Il delitto di trattamento illecito dei dati personali*, Torino, 2012, p. 134.

[72] La clausola di riserva era ben presente sia nella previgente formulazione dell'articolo che nel testo dell'art. 35 della L.677/96 con la quale, come si è già visto, la disposizione si poneva in evidente continuità normativa.

[73] Si avrebbe quindi un ampliamento applicativo rispetto alla previgente normativa che identificava il soggetto agente solo con il titolare, il responsabile del trattamento oppure la persona designata ex art 2 *terdecies.*

[74] Parere sullo schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679, cit., § 1.4.

Sulla introduzione del requisito nocumento, quale elemento della fattispecie, occorre necessariamente soffermare l'attenzione, poiché la dottrina è pressoché concorde nel ritenere che tale requisito sia stato lo strumento attraverso il quale è stato possibile delimitare l'area del penalmente rilevante alle condotte connotate da maggiore offensività[75] .

La figura del nocumento era in realtà già presente anche nella formulazione originaria dell'art. 167, nell'ambito del quale tuttavia rivestiva il diverso ruolo di condizione obiettiva di punibilità intrinseca[76] , mentre nel testo attuale esso viene inquadrato come l'evento stesso del reato ("*chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato ... arreca nocumento all'interessato*)[77] e ne consegue pertanto che l'evento dannoso deve ora essere espressamente previsto e voluto dall'autore della condotta.

Si tratta quindi di una impostazione del tutto nuova in cui la punibilità non è più sottoposta al verificarsi di una mera condotta in violazione di precetti extra penali, bensì alla volontaria infrazione dei medesimi[78].

---

[75] Così S. ORLANDO, *I limiti della tutela penale del trattamento illecito dei dati personali nel mondo digitale*, in *Diritto penale contemporaneo*, 2, 2019, 178-200; L. D'AGOSTINO, *Commento al D.lgs.10.08.2018 n.101*, in *Archivio penale*, 1, 2019, 1-58, p. 31.

[76] Nella previgente disposizione una parte della dottrina argomentava proprio partendo dalla coincidenza fra dolo specifico e nocumento per far rientrare quest'ultimo fra le condizioni di punibilità intrinseche; A. MANNA, *Il quadro sanzionatorio penale e amministrativo del codice sul trattamento dei dati personali*, cit., p. 747; A. MANNA, M. DI FLORIO, *Riservatezza e diritto alla privacy: in particolare la responsabilità per omissionem dell'internet provider*, in *Cybercrime*, (a cura di CADOPPI, CANESTRARI, MANNA, PAPA), Milano, 2019, p. 897.

[77] Sul nocumento quale elemento del reato si veda Cass. pen 3^, 29.03.2019 n.917: "*come chiarito dalla giurisprudenza di questa Corte, nel reato di trattamento illecito di dati personali previsto dall'art.167 in esame il nocumento è costituito dal pregiudizio, anche di natura non patrimoniale, subito dalla persona cui si riferiscono i dati quale conseguenza dell'illecito trattamento (Sez. 3, n. 29549 del 7/2/2017, F, Rv. 270458, citata in sentenza). Nella citata pronuncia viene ricordato come, in un primo tempo, la giurisprudenza abbia qualificato il verificarsi del nocumento quale condizione oggettiva di punibilità "intrinseca", che attualizza l'offesa dell'interesse tutelato già realizzata dal fatto tipico (Sez. 3, n. 7504 del 16/7/2013, dep. (2014), Pontillo, Rv. 259261; Sez. 5, n. 44940 del 28/9/2011, C. e altro, Rv. 251448; Sez. 3, n. 16145 del 5/3/2008, P.C. in proc. Amorosi e altro, Rv. 239898; Sez. 3, n. 28680 del 26/3/2004, Modena, Rv. 229465), il quale costituirebbe una fattispecie di pericolo concreto, integrata dalla condotta di trattamento assistita dal dolo specifico, punibile solo a condizione del verificarsi del predetto accadimento, mentre, più recentemente, il nocumento è stato ritenuto un elemento costitutivo del reato, avuto riguardo alla sua omogeneità rispetto all'interesse leso e alla sua diretta derivazione causale dalla condotta tipica, con conseguente necessità che esso sia previsto e voluto o, comunque, accettato dall'agente come conseguenza della propria azione, indipendentemente dal fatto che costituisca o si identifichi con il fine dell'azione stessa (Sez. 3, n. 40103 del 5/2/2015, Ciulla, Rv. 264798)".*

[78] Ad avviso di una corrente di pensiero tuttavia indicare il danno quale fine del soggetto agente presenta un profilo di indeterminatezza perché - a meno che non si voglia attribuire significati differenti ai termini danno e nocumento - in questa maniera l'oggetto del dolo specifico coincide parzialmente con quello del dolo generico. Secondo questo orientamento infine si potrebbe trattare di due fattispecie di reato alternative, una definita dallo scopo lucrativo e con il dolo generico di nocumento anche nella forma del dolo eventuale ed un'altra in cui invece la finalità

Ad avviso di una corrente di pensiero, nella fattispecie in esame, si ravvisa una ipotesi di dolo specifico apparente. Ed infatti, per la presenza del dolo generico l'agente deve infatti rappresentarsi e volere gli elementi del fatto tipico (ossia le singole violazioni delle leggi extrapenali cui fa riferimento l'art.167 nonché lo stesso nocumento alla persona offesa che si realizzerà concretamente), mentre - per la sussistenza del dolo specifico di danno o di profitto - il soggetto dovrà avere una ulteriore volizione rispetto a quella già orientata sugli elementi tipici del fatto reato, ovvero la mera intenzione, la finalità lucrativa o di profitto che non occorre venga materialmente realizzata per l'integrazione del fatto reato[79] .

Secondo questa posizione dottrinale si evidenzia quindi una similitudine nella struttura della fattispecie in esame ed il reato di patrocinio e consulenza infedele di cui all'art. 380 c.p., che appare costruita tramite la medesima tecnica normativa, ovvero un reato di evento il cui fulcro sia il nocumento agli interessi della parte ed al cui verificarsi viene ricollegata l'offesa.

È significativo che anche in questo caso si tratterebbe di una norma posta a salvaguardia di un interesse complesso, comprensivo sia dell'interesse privato che del diverso interesse pubblicistico al regolare funzionamento della giustizia.

Anche nel caso del trattamento illecito di dati personali ci troveremmo pertanto dinanzi ad una fattispecie delittuosa in cui l'offesa penalmente rilevante riaffiora solo quando, al di là della lesione del bene individuale, venga offesa o comunque posta in pericolo anche la globale struttura di salvaguardia della riservatezza[80].

È possibile quindi, ad una sommaria valutazione, concludere che l'obiettivo del legislatore sia effettivamente stato quello di delineare una fattispecie delittuosa applicabile solo ai casi di effettiva rilevanza.

In merito, occorre invece prendere atto dell'orientamento assolutamente estensivo della giurisprudenza che, in tema di trattamento illecito dei dati, si è invece allineata su una applicazione costante della fattispecie anche ad ipotesi di non rilevante gravità, grazie anche alla elaborazione di una nozione di nocumento particolarmente ampia, ricomprensiva in sostanza di qualsiasi tipo di pregiudizio giuridicamente rilevante, di qualsiasi natura, patrimoniale e non patrimoniale[81].

---

dell'agente, coincidendo con l'oggetto del dolo generico lo qualifica piuttosto come dolo intenzionale; così V. MANES, F. MAZZACUVA, cit., p. 173.

[79] Si tratta di una "mera intenzione" proprio in quanto è diretta ad una finalità la cui attuazione concreta non è però necessaria all'integrazione della fattispecie; così S. ORLANDO, cit., p. 192.

[80] Così S. ORLANDO, cit., p.191.

[81] Cass. Pen. III sez. penale, n.20013/2019: "*Per la consumazione del reato di trattamento illecito di dati personali di cui al secondo comma dell'art. 167 d.lgs. 196/2003, è richiesto che la volontà del soggetto agente sia connotata dal porsi lo scopo ulteriore – alternativamente – del profitto (anche in vantaggio di terzi) o del danno, pur non occorrendo che tale fine venga effettivamente conseguito. Quanto all'elemento del "nocumento", con tale locuzione deve intendersi un pregiudizio giuridicamente rilevante di qualsiasi natura patrimoniale o non patrimoniale, subito dal soggetto passivo".*

3.2. Le nuove fattispecie speciali di trattamento illecito:167 bis e 167 ter Codice Privacy

Oltre alla fattispecie - già esaminata - contemplata nel comma 3 dell'art. 167, il complessivo sistema di tutela dei dati personali è stato ulteriormente rafforzato tramite l'inserimento di due norme di nuova formulazione, appositamente predisposte per la salvaguardia di quelle che sembrano essere le ipotesi più offensive di attacco alla riservatezza, ovverosia la comunicazione e diffusione dei dati in violazione degli artt. 2 *ter,* 2 *sexies* e 2 *octies* del Codice, nonché l'acquisizione con mezzo fraudolento di dati personali oggetto di trattamento su larga scala e presenti in un archivio automatizzato o in una parte sostanziale di esso.

Si tratta - ad avviso di chi scrive - di una struttura costituita da tre parti autonome ma comunque complementari, costituenti dunque un trittico; la disposizione centrale è rappresentata evidentemente dal già esaminato trattamento illecito dei dati così come ridelineato dalla novella, che non ha in realtà visto grandi mutamenti sotto il profilo della pena rispetto al testo previgente, cui sono state però affiancate due nuove ipotesi di reato, in cui viene sostanzialmente integrata la medesima tipologia di condotta ma aggravata in ciascuna ipotesi da elementi che giustificano l'innalzamento della pena.

Anche in questo caso, tuttavia, le singole disposizioni non appaiono pienamente soddisfacenti sotto il profilo della chiarezza e della determinatezza; in particolare, per quanto attiene l'art.167 *bis*, si tratta di norma il cui testo ha visto più modifiche nel corso dei lavori preparatori ed il cui obiettivo, nelle intenzioni del legislatore, dovrebbe essere il freno alla costituzione ed alla diffusione di ampi database privati a fini commerciali, quando effettuati con modalità non regolari. A tal fine, nel primo comma viene sanzionato con la reclusione da uno a sei anni chiunque, al fine di trarre profitto per sé o per altri, comunichi o diffonda un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-*ter* (relativo ai trattamenti effettuati per l'esecuzione di un compito di interesse pubblico) 2-*sexies* (con riferimento ai trattamenti di categorie particolari di dati personali necessari per motivi di interesse pubblico) nonché 2-*octies* (per i trattamenti di dati relativi a condanne penali e reati); nel secondo comma viene di fatto prevista la medesima condotta, caratterizzata però dalla assenza di consenso degli aventi diritto.

La fattispecie è stata delineata come reato comune ("chiunque") sia nel primo che nel secondo comma, su sollecitazione sia del Garante che della Commissione parlamentare[82]; la previsione del massimo edittale superiore, nel massimo, a cinque anni di reclusione consente sia l'applicazione delle misure custodiali che la possibilità di intercettazioni ai sensi dell'art. 266 comma 1 lett.a. c.p.p.

[82] Rispetto al primo schema di decreto legislativo sottoposto alla Commissione Parlamentare la disposizione è stata modificata anche nella rubrica, ove il testo originario riportava il delitto di "Comunicazione e diffusione illecita di dati personali riferibili ad un numero rilevante di persone".

Per quanto attiene alla condotta delittuosa di comunicazione e diffusione[83], il riferimento alle definizioni di "archivio automatizzato" nonché alla "parte sostanziale" dello stesso hanno dato luogo a più di un dubbio interpretativo, come pure il ricorso alla ancor più ampia indicazione del "trattamento su larga scala" che ha sostituito nel testo definitivo la definizione prima proposta che faceva invece riferimento ad un "rilevante numero di persone"; nel codice privacy non si rinviene alcun riferimento espresso alla nozione di archivio automatizzato, mentre nel Regolamento Europeo la nozione di "archivio" viene invece fornita dal sesto comma dell'art. 4, con riferimento a "*qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico".*

Anche la definizione di "parte sostanziale di un archivio automatizzato" è certamente foriera di più di una difficoltà di lettura a causa della assoluta genericità del termine, che neppure consente di comprendere se il riferimento alla concreta valenza dello stesso sia da intendere in senso quantitativo o piuttosto qualitativo[84].

Ancor più oscura è la definizione ed il concetto stesso di "larga scala", in ordine al quale almeno sembra si possa limitare il significato concreto ad una valenza esclusivamente quantitativa.

L'unico riferimento immediato si rinviene nel considerandum n. 91 del G.D.P.R. sulla valutazione d'impatto, che fa uso del termine: "*Ciò dovrebbe applicarsi in particolare ai trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un*

[83] Definizioni queste espressamente previste nell'art. 2 ter comma 4 del Codice, ove si intende per:

a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-*quaterdecies*, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Tuttavia secondo D'AGOSTINO non è detto che il legislatore abbia effettuato un rinvio tacito all'art. 2 ter, perché "la collocazione sistematica della definizione lascia dunque supporre che la condotta di comunicazione e diffusione di cui all'art.167-*bis* possa assumere significato 'normativo' soltanto con riferimento all'illecito trattamento di dati effettuato in violazione dell'art. 2-ter, giusto il rinvio ad esso operato dalla disposizione incriminatrice"; così L. D'AGOSTINO, *Commento al D.lgs 10.08.2018 n.101*, cit., p. 46.

[84] Secondo una voce dottrinale l'attributo "automatizzato" potrebbe rinviare al fenomeno ben noto della profilazione, cui fa riferimento anche l'art. 22 del Regolamento, ove si specifica che " *l'interessato ha il diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*"; così ORLANDO S., op. cit. p.195, che ravvisa però un profilo di incostituzionalità su tutta la fattispecie per violazione del principio di tassatività e determinatezza del precetto con riferimento al principio di tassatività.

vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti".

Il terzo comma dell'articolo contiene poi disposizioni procedurali che riportano al medesimo meccanismo di coordinamento tra la Procura ed il Garante, cui si è già fatto cenno in tema di trattamento illecito di dati personali.

Non meno complessa appare la lettura dell'art. 167 *ter*, propriamente attinente alla condotta di chiunque, al fine di profitto o per arrecare ad altri un danno, in questo caso invece acquisisca con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso, contente dati personali oggetto di trattamento sul larga scala; in questa nuova fattispecie delittuosa, la cornice edittale è la reclusione da uno a quattro anni, quindi si presenta meno afflittiva rispetto alla parallela fattispecie già esaminata di cui all'art. 167 bis.

La condotta commissiva prevista dall'art. 167 *ter* è la acquisizione[85] di dati personali pur sempre contenuti in un archivio automatizzato (o in parte sostanziale dello stesso) ed oggetto di trattamento su larga scala.

Si tratta pertanto di un reato comune di pura condotta, indipendente dal nocumento effettivo, perfettamente integrato dalla mera acquisizione dei dati e comunque contemperato sul versante soggettivo dalla previsione del dolo specifico alternativo di profitto e di danno, al fine di circoscrivere adeguatamente l'incriminazione alle condotte concretamente lesive; esso viene pacificamente qualificato quale reato plurioffensivo posto a difesa tanto della privacy individuale quanto del patrimonio del proprietario dell'archivio[86].

E' opinione concorde della dottrina che nelle due fattispecie di cui agli artt. 167 *bis e te*r il bene da salvaguardare non sia *in primis* la riservatezza informatica, quanto piuttosto l'interesse generale della collettività ad un utilizzo dei sistemi informatici digitali - e quindi dei dati personali in essi contenuti - che sia conforme alle normative vigenti, nella prospettiva che solo un uso illegittimo di strumenti potenzialmente tanto offensivi

[85] Non si rinviene alcuna indicazione espressa su cosa si debba intendere per "acquisizione" nel Regolamento Europeo; sulla inusuale scelta del termine "acquisire" si veda anche D'Agostino, il quale rileva condivisibilmente come il termine possa essere inteso con il significato di "procurarsi la disponibilità" dell'archivio o di una parte sostanziale di esso, ma non può ricomprendere tuttavia il diverso caso in cui l'agente raccolga illecitamente dati e solo successivamente li organizzi in un archivio; per questo motivo la cosiddetta "autoproduzione" di un archivio non potrà rientrare per parte sua nell'ipotesi delineata dall'art. 167 ter ma, solo nel caso di diffusione dell'archivio stesso, nella diversa fattispecie di cui invece all'art. 167 bis; qualora poi venga illegittimamente acquisito un archivio e poi diffuso, l'agente risponderà sia per la fattispecie dell'art.162 bis quanto per quella dell'art.162 ter, ravvisandosi in questo caso una ipotesi di concorso materiale di reati. L. D'AGOSTINO, *Commento al D.lgs 10.08.2018*, cit. p. 47

[86] Conforme, L. D'AGOSTINO, *Commento al D.lgs. 10.08.2018*, cit. p. 47.

possa giustificare il ricorso alla sanzione penale piuttosto che il presidio della tutela amministrativa.

Nel terzo comma dell'articolo in esame si trova nuovamente il rinvio allo stesso meccanismo di coordinamento fra Garante ed Autorità giudiziaria previsto dai commi 4 e 5 per il trattamento illecito dei dati, nonchè l'attenuante specifica di cui all'art.167 comma 6.

3.3. Considerazioni sugli articoli 168, 170, 171, 172 D.lgs. 137/2006

L'ipotesi delittuosa di cui all'art.168 del Codice Privacy - pur rimasta quale norma a presidio delle funzioni della Autorità di settore - è stata tuttavia rivista dal legislatore delegato sin dalla rubrica della norma, ora rinnovata in "*Falsità nelle dichiarazioni al Garante ed interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*".

La novella ha quindi eliminato il richiamo alle comunicazioni previste nell'abrogato art. 32 *bis* commi 1 e 2 del Codice Privacy (Adempimenti conseguenti ad una violazione di dati personali)[87] come pure le notificazioni del trattamento che venivano imposte dall'art. 37 per alcune tipologie di dati, anch'esso ora abrogato[88].

---

[87] Il riferimento è alle comunicazioni cui è tenuto il titolare del trattamento in caso di violazione dei dati ai sensi degli art. 33 e 34 del GDPR (ora sottoposte alle sanzioni di cui all'art.83 par. 4 del Regolamento) nonché degli art. 26 e 27 del D.lgs. 18.5.2018 n. 51 relativo al trattamento dei dati personali ai fini della prevenzione dei reati. L'art. 32 *bis* sugli "Adempimenti conseguenti ad una violazione di dati personali" venne inserito nel Codice Privacy tramite il D.lgs. 69/2012, in attuazione della Direttiva 2009/136/CE e - parallelamente - venne anche modificato l'art. 168 Codice Privacy con cui veniva appunto sanzionata la falsità nelle comunicazioni ex art. 32 bis; si vedano anche, per le comunicazioni dei Data Breach, l'art. 14 della Direttiva NIS 2016/11848/UE del 6.07.2016 del Parlamento europeo e del Consiglio, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi, cui è stata data attuativa in Italia tramite il D.lgs 18.5.2018 n.65, in vigore a far data dal 26.06.2018, nonché dal Regolamento UE n.910/2014 eIDAS (Electronic IDentification Authentication and Signature) sull'identità digitale. Per una compiuta disamina degli obblighi del titolare del trattamento in caso di Data Breach si veda M. LUBERTO, *Gli obblighi dei fornitori di servizi di comunicazione elettronica in caso di violazione dei dai personali (Data breach) ed il delitto dell'art.168 D.lgs 196/2003*, in *Cybercrime*, (a cura di CADOPPI, MANNA, FIORIO CANESTRARI), Milano, 2019.

[88] Si riporta, in tal senso, il considerandum n.89 del G.D.P.R. per cui "*La direttiva 95/46/CE ha introdotto un obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali. Mentre tale obbligo comporta oneri amministrativi e finanziari, non ha sempre contribuito a migliorare la protezione dei dati personali. È pertanto opportuno abolire tali obblighi generali e indiscriminati di notifica e sostituirli con meccanismi e procedure efficaci che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità. Tali tipi di trattamenti includono, in particolare, quelli che comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale*".

Nella disposizione ora vigente vengono previste nel primo comma due distinte fattispecie di reato ostativo, caratterizzate dal dolo generico ed entrambe riconducibili al "mendacio documentale": salvo che il fatto non costituisca più grave reato, chiunque dichiari od attesti falsamente notizie o circostanze oppure produca atti o documenti non veritieri in un procedimento o nel corso di un accertamento dinanzi al Garante, verrà punito con la reclusione da sei mesi sino a tre anni[89]; al di fuori dei casi indicati nel primo comma dell'articolo, la sanzione penale per le più ampie fattispecie di turbativa - introdotte invece ex novo dal secondo comma - arrecata da chi intenzionalmente cagioni un'interruzione oppure alteri la regolarità di un procedimento dinanzi al Garante o degli accertamenti svolti dallo stesso, è invece della reclusione sino ad un anno[90].

Per quanto attiene alle due ipotesi di reato comune di cui al primo comma la condotta di falsa attestazione o dichiarazione può essere realizzata con qualsiasi mezzo, mentre non vi è accordo in dottrina se la disposizione faccia riferimento alle sole ipotesi di falso ideologico oppure anche di falso materiale[91].

Con riferimento alle nuova tipologie delittuose di turbativa, occorre rilevare come l'interruzione presupponga che si sia cagionata una inattività, anche temporanea, da parte della Autorità di controllo, mentre la definizione di turbamento della regolarità procedimentale rimanda piuttosto ad un non corretto funzionamento della stessa, il quale venga cagionato da una condotta intenzionale del soggetto agente; detta condotta dovrà quindi necessariamente essere posta in essere con la precipua volontà di rallentare o comunque creare difficoltà al corretto andamento della procedura di controllo.

L'unica effettiva ipotesi di depenalizzazione disposta dalla normativa di adeguamento - in linea con la nuova impostazione adottata dal Regolamento ed incentrata tutta sul momento della prevenzione nella tutela dei dati personali - ha riguardato l'art. 169 in tema di misure minime di sicurezza,[92] già previste dall'abrogato art. 33 del D.lgs. 196/03[93]; sul

[89] Si tratta della stessa pena prevista dal testo dell'art. 168 anteriore alla novella.

[90] Si ritiene sia una ipotesi speciale rispetto al delitto di cui all'art. 340 c.p. (interruzione di un ufficio o servizio pubblico o di un servizio di pubblica necessità) da cui si differenzia per il dolo intenzionale; così V. MANES, L. MAZZACUVA., cit, pag 175.

[91] Cfr. A. MASSARO A, *Commento all'Art. 168, "*Codice Privacy. Commento al D.lgs. 30 giugno 2003 n.196 e al D.lgs 10.08.2018 n.101 alla luce del Regolamento (UE) 2016/679 (GDPR)", Pisa, 2019, (a cura di R. SCIAUDONE, E. CARAVÀ), p. 909.

[92] Sulla opportunità di una depenalizzazione si erano già espressi A. MANNA A., M. DI FIORIO, *Riservatezza e diritto alla privacy: in particolare, la responsabilità per omissione dell'Internet Provider,* in Cybercrime, Cap-XXII.

[93] Il vecchio testo dell'articolo 33 imponeva l'adozione di minime misure idonee, ora sostituite da misure tecniche ed organizzative frutto di una valutazione personalizzata che dovrà essere predisposta dal titolare del trattamento in fase progettuale; in particolare, secondo il disposto dell'art. 24 GDPR, «*tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*» ed ancora, dell'art. 32 per cui «*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e*

punto, occorre rammentare che l'art. 24 del decreto di adeguamento estende l'applicazione delle sanzioni amministrative previste dal G.D.P.R. in sostituzione di quelle penali anche alle violazioni commesse anteriormente alla entrata in vigore del decreto stesso, a meno che il procedimento penale non risulti già definito con sentenza o decreto già passato in giudicato: in tal caso sarà il giudice dell'esecuzione a dover provvedere alla revoca della sentenza o del decreto perché il fatto non è più previsto dalla legge come reato.

In ossequio al generale principio del *favor rei*, il terzo comma dell'art. 24 prevede comunque che ai fatti commessi anteriormente alla vigenza del decreto attuativo non possa essere applicata una sanzione amministrativa pecuniaria per un importo superiore nel massimo alla pena originariamente prevista per il reato abrogato, con riferimento al ragguaglio tra pene detentive e pecuniarie di cui all'art 135 del Codice Penale, e non si applicano le sanzioni amministrative accessorie introdotte dallo stesso decreto attuativo, a meno che queste non sostituiscano corrispondenti pene accessorie.

La controversa disposizione di cui all'art. 170, riferita all' inosservanza dei provvedimenti del Garante, sanziona con la reclusione da tre mesi a due anni chiunque, pur essendovi tenuto, non osservi il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2 *septies*, comma 1, nonché i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'art.13 della legge 25 ottobre 2017, n. 163.

La disposizione è stata reintrodotta nello schema definitivo di decreto dopo essere stata sottoposta a parere parlamentare, anche in considerazione del trattamento di rigore disposto invece a livello comunitario.

Anche se la norma sembra delineare un reato comune ("chiunque"), questa violazione potrà essere concretamente posta in essere solo dal destinatario delle tipologie di provvedimenti elencati nella stessa, ovvero:

- l'art. 58 par. 2 lett. F) del GDPR, ossia la violazione dei provvedimenti con cui il Garante e ogni altra Autorità riconosciuta impongano una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;

- l'art. 2 *septies* del GDPR, ovvero l'inosservanza dei provvedimenti del Garante attinenti le autorizzazioni al trattamento dei dati genetici, biometrici e relativi alla salute;

- l'art. 21 del D.lgs. 101/2018 con riferimento alle autorizzazioni generali con cui il Garante "individua le prescrizioni contenute nelle autorizzazioni generali già adottate, relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 2, lettera b) e 4, nonché al capo IX del regolamento (UE) 2016/679, che risultano compatibili con le disposizioni del medesimo regolamento e del presente decreto e, ove occorra, provvede al loro aggiornamento"[94].

le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio».

[94] Sui profili di criticità della disposizione, rilevati in tema di rispetto della riserva di legge si veda V. MANES, F. MAZZACUVA, cit., p. 176.

L'art. 171 del Codice Privacy è stato solo parzialmente riformulato: a fronte della versione anteriore rispetto alla novella legislativa, ove la violazione delle disposizioni di cui all'articolo 113 e dell'art 4 primo e secondo comma della L. 300/1970 (Statuto dei lavoratori) veniva punita con le sanzioni di cui all'art. 38 del medesimo testo normativo, l'attuale disposizione (la cui rubrica espressamente ora richiama le violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori) ribadisce l'applicazione delle contravvenzioni di cui all'articolo 38, con riferimento però all'inosservanza del disposto di cui all'art. 4 comma 1 ed 8 [95] dello Statuto dei lavoratori, quindi a tutte quelle infrazioni che siano attinenti all'impiego di strumenti che consentano il controllo a distanza dei lavoratori quando dette verifiche non siano dovute ad esigenze lavorative o di produzione, oppure che siano connesse all'omissione delle procedure sindacali od amministrative previste per l'installazione degli impianti.

Infine, l'art. 172 (pene accessorie) è stato unicamente integrato con l'espresso riferimento alla norma del codice penale che prevede la sanzione accessoria della pubblicazione della sentenza in caso di condanna per uno dei delitti previsti dalla normativa in vigore.

4. Un'occasione perduta? La responsabilizzazione dell'ente con riferimento ai privacy crimes

All'indomani dell'entrata in vigore del decreto di adeguamento al Regolamento Europeo, parte della dottrina non ha mancato di rilevare come il Legislatore ben avrebbe potuto inserire, con l'occasione, le fattispecie criminose in tema di illecito trattamento dei dati nel novero dei reati presupposto per la responsabilità diretta delle persone giuridiche di cui al D.Lgs 231/2001[96]: giacché il testo normativo che disciplina la responsabilità

[95] L.20.5.1970 n.300 Art. 4 (Impianti audiovisivi)

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

[96] Così D'AGOSTINO L., *Commento al D.lgs. 10.08.2018 n.101,* cit., p. 171; M. LAMANNUZZI, *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE*, in *JusOnLine* 1/2017, 218-265 p. 257; V. ARAGONA, *Corporate liability e compliance in the cyber privacy crime; il nuovo modello organizzativo privacy",* in *La tutela penale della privacy nel cyberspazio*,

amministrativa dell'ente prevede una disposizione apparentemente dedicata ai delitti informatici nonché al trattamento illecito di dati (art. 24 *bis*) nel cui testo, tuttavia, non è dato ravvisare - allo stato - alcuna delle fattispecie propriamente previste a difesa della riservatezza informatica[97].

Effettivamente, anche ad una prima lettura[98] emergono diverse affinità tra la struttura organizzativa predisposta dal Regolamento a salvaguardia del dato personale ed il modello di *compliance* delineato dalla normativa nazionale in tema di responsabilità amministrativa degli enti, a cominciare dalla rigida adozione di serrati modelli organizzativi basati sulla gestione del rischio. Spostando l'asse del sistema normativo sulla protezione preventiva dei dati *by design and by default*[99] il Regolamento ha adottato una metodologia organizzativa basata sulla prevenzione del trattamento illecito, in cui primaria importanza assumono la figura del DPO (Data Protection Officer), ovvero il responsabile del trattamento dei dati che richiama, per struttura e funzioni, l'Organismo di Vigilanza previsto dal modello organizzativo 231[100] nonché la Valutazione d'impatto sulla protezione dei dati (DPIA) prevista dall'art.35 il cui parallelo riferimento sembra essere il ovvero il modello organizzativo di prevenzione di cui agli artt. 6 e 7 del D.lgs 213/2001[101].

2-2019, 251-265; C. CUPELLI, R. FICO, *I riflessi penalistici del Regolamento UE 2016/679 e le nuove fattispecie di reato previste nel Codice Privacy dal d.lgs. n. 101/2018*, *I dati personali nel diritto europeo* (a cura di V. CUFFARO , R. RICCIUTO, R. D'ORAZIO), 1107-1125.

[97] L'art. 24 *bis* è stato inserito nel D.Lgs. 231/2001 dall'art.7 della legge 18.03.2008 n.48, che ha ratificato la Convenzione di Budapest del 23 novembre 2001 del Consiglio d'Europa sulla criminalità informatica, il primo accordo internazionale riguardante i crimini commessi attraverso internet o altre reti informatiche; l'articolo era stato poi integrato dall'art. 9 del dl.14.08.2013 n. 93, recante "Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province" con il richiamo ai reati di cui agli art. 640-*ter* c.p. (frode informatica); art. 55, comma 9, del D.Lgs. 21 novembre 2007, n. 231 (utilizzo indebito e falsificazione di carte di credito); artt. 167, 168 e 170 del D.Lgs. 196/2003 (illecito trattamento di dati, falsità nelle dichiarazioni e notificazioni al Garante, e inosservanza di provvedimenti del Garante), ma in sede di conversione in legge è stato eliminato il secondo comma dell'art.9, probabilmente a ragione del potenziale impatto che la disposizione avrebbe potuto avere in sede applicativa nei confronti delle società commerciali.

[98] C. CUPELLI, R. FICO, *I riflessi penalistici del Regolamento UE 2016/679 e le nuove fattispecie di reato previste nel Codice Privacy dal d.lgs. n. 101/2018*, cit., 1107-1125

[99] In merito alla valorizzazione del momento della prevenzione nel GDPR, si veda V. ARAGONA, *Corporate liability e compliance in the cyber privacy crime; il "nuovo modello organizzativo privacy,* in *La tutela penale della privacy nel Cyberspazio*, *Diritto penale contemporaneo*, 2-2019, pp. 177-266

[100] Sulla non sovrapponibilità delle due figure si veda tuttavia Aragona, secondo cui "OdV sorveglia il modello organizzativo “dall’esterno” senza entrare nello stesso, il DPO, invece, riveste anche una funzione consultiva, che determina una sua maggiore ingerenza nella *compliance* in materia di *privacy*. Inoltre, le valutazioni operate dal DPO hanno un riferimento positivo quale il Codice *privacy* e il GDPR, a differenza dell’OdV, che ha a riferimento il modello organizzativo e la sua adeguatezza preventiva. " V. ARAGONA, cit., p. 262.

[101] C. CUPELLI - R. FICO, *I riflessi penalistici del Regolamento UE 2016/679 e le nuove fattispecie di reato previste nel Codice Privacy dal d.lgs. n. 101/2018*, cit., pp. 1113-1114; secondo questa dottrina DPIA ed i modelli *ex* art. 6 e 7 d.lgs. n.231/2001 condividono la medesima logica di

Si rileva altresì come sia nell'ambito del Regolamento Privacy che nella disciplina della responsabilità da reato degli enti venga posta particolare attenzione al fenomeno del Whistle blowing: l'art.6 del D.Lgs. 231/2001 è stato integrato con norme di tutela in favore dei dipendenti e collaboratori che abbiano segnalato illeciti di cui siano venuti a conoscenza nell'ambito della propria attività lavorativa e che dovranno essere opportunamente garantiti da atti discriminatori o comunque ritorsivi e il decreto attuativo del regolamento europeo è, per parte sua, intervenuto sul codice privacy attraverso l'art. 2 *undecies* comma 1 lettera f), per effetto del quale i diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento, qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio[102].

Alla luce quindi dei rilevati punti di contatto, è stata conclusione pressoché unanime della dottrina che sarebbe conseguentemente stato auspicabile un coordinamento legislativo tra i due modelli organizzativi al fine di introdurre un unico modello integrato di tutela dei dati personali in ambito aziendale.

5. Il trattamento dei dati personali per fini di prevenzione e repressione penale: problemi di coordinamento

Tramite il D.Lgs. n. 51/2018 è stata poi data attuazione alla Direttiva UE 2016/680, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, che ha abrogato la decisione quadro 2008/977/GAI del Consiglio[103].

La Direttiva - come il Regolamento - richiedeva agli Stati Membri l'introduzione di sanzioni *effettive, proporzionate e dissuasive*; con l'art. 11 della Legge delega 163/2017 veniva indicato quale criterio direttivo specifico da seguire per l'attuazione della direttiva - oltre ai criteri direttivi di cui all'art.1, comma 1 - la previsione, da parte dell'esecutivo, dell'applicazione della pena detentiva non inferiore nel minimo a sei mesi e non superiore nel massimo a cinque anni per le violazioni delle disposizioni adottate a norma della

verifica preventiva, attuata mediante l'analisi di ogni possibile conseguenza negativa del processo sulla quale poi deve essere strutturata una misura preventiva *ad hoc*, così da scongiurarne la possibilità di accadimento; analogamente a quanto accade per il modello di gestione del rischio 231, anche con la DPIA occorre però procedere ad un opportuna valutazione del bilanciamento degli interessi contrapposti nella gestione dei dati.

[102] Sul punto, ARAGONA, cit., p. 262.

[103] La decisione quadro 2008/977/GAI del Consiglio del 27.11.2008 venne emanata nell'ambito del Terzo Pilastro, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale; bisogna però rammentare come fosse applicabile al solo trattamento dei dati tra Stati Membri e non quindi sui trattamenti effettuati dai singoli Stati al proprio interno.

direttiva stessa, ferma restando la disciplina vigente per le fattispecie penali già oggetto di previsione.

Il Decreto legislativo n.51 del 18 maggio 2018 - entrato in vigore l'8 giugno 2018 - ha quindi rivisto interamente la disciplina del trattamento dei dati personali in ambito penale, sostituendo in gran parte la previgente normativa di cui alla parte seconda del Codice Privacy, ai titoli primo (Trattamenti in ambito giudiziario) e secondo (Trattamenti da parte delle forze di Polizia), dedicati a specifici settori.

Nel capo VI del decreto legislativo, dedicato appunto agli illeciti penali, sono state quindi introdotte nuove fattispecie; si tratta delle ipotesi di Trattamento illecito dei dati (art. 43)[104], Falsità in atti e dichiarazioni al Garante (art.44)[105], Inosservanza dei provvedimenti del Garante (art.45)[106]; l'art. 46 infine stabilisce che la "condanna per uno dei delitti previsti dal presente decreto importa la pubblicazione della sentenza, ai sensi dell'articolo 36, secondo e terzo comma, del codice penale".

La dottrina[107] non ha mancato di rilevare come, in questo caso, la coerenza complessiva del sistema sanzionatorio abbia purtroppo scontato la sfasatura temporale con la quale la legislazione interna è stata adeguata alle fonti comunitarie[108]; la normativa riprende interamente le disposizioni previgenti del Codice Privacy, con alcune incoerenze rispetto quindi alla disciplina attualmente in vigore; non di poco rilievo appare infatti l'osservazione per cui, a parte le singole fattispecie che non appaiono in linea con le evoluzioni interpretative della giurisprudenza, nel decreto attuativo manca una norma di coordinamento ove si specifichi che le disposizioni penali di cui al Codice Privacy non si

[104] *Art. 43 Trattamento illecito di dati*

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per se' o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dall'articolo 5, comma 1, è punito, se dal fatto deriva nocumento, con la reclusione da sei mesi a un anno e sei mesi o, se la condotta comporta comunicazione o diffusione dei dati, con la reclusione da sei mesi a due anni.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per se' o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dall'articolo 7 o dall'articolo 8, comma 4, e' punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

[105] *Art. 44. Falsità in atti e dichiarazioni al Garante*

1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante riguardante il trattamento dei dati di cui all'articolo 1, comma 2, o nel corso di accertamenti riguardanti i medesimi dati, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni.

[106] *Art. 45. Inosservanza di provvedimenti del Garante*.

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi dell'articolo 58, paragrafo 2 lettera F, comma 2, del Regolamento UE 2016/679, in un procedimento riguardante il trattamento dei dati di cui all'art.1 comma 2 è punito con la reclusione da tre mesi a due anni.

[107] Così MANES V.- MAZZACUVA F., *GDPR e nuove disposizioni penali del Codice Privacy*, "Diritto penale e processo", 2/2019, 171-179, p. 179.

[108] Il D.Lgs. n. 51/2018 è stato pubblicato in Gazzetta Ufficiale il 24 maggio 2018 ed è quindi anteriore rispetto all'entrata in vigore del D.lgs. 101/2018, ma la premura è stata in questo caso dettata dall'approssimarsi del termine di scadenza della direttiva.

applicano ai trattamenti previsti invece nel decreto legislativo 51/2018[109] il che potrebbe comportare per alcune ipotesi di trattamento illecito la possibilità di duplice qualificazione penale[110].

6. Qualche breve riflessione conclusiva

Da questa breve disamina si può constatare come, in realtà, la disciplina ed il modello organizzativo stesso del Regolamento sembrano essere ideato precipuamente per enti di grandi dimensioni ed è - ad avviso di chi scrive - una criticità di non poco peso, giacchè saranno verosimilmente le piccole e medie imprese ad affrontare con maggiore difficoltà l'adeguamento alle previsioni della normativa privacy, nonostante l'art 40 del GDPR nel primo comma inviti gli Stati Membri, le autorità di controllo, il comitato e la Commissione ad incoraggiare l'elaborazione di codici di condotta "destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese ".

In merito, non ci si può esimere dal rilevare la complessità della normativa derivante dalla tecnica di redazione prescelta, che rende la disciplina di difficile comprensibilità ai fini concretamente applicativi.

La scelta legislativa si è orientata per una soluzione di compromesso, per cui, venuta meno l'ipotesi della depenalizzazione si è preferito circoscrivere le fattispecie delittuose in maniera tale da consentirne l'applicazione ai soli casi di rilievo; nella prospettiva di una tutela multilivello la salvaguardia del dati nella generalità dei casi dovrebbe essere affidata alla Autorità di controllo, riservando l'intervento della Autorità giudiziaria nelle sole ipotesi di effettiva gravità; per quanto attiene il sistema di coordinamento tra il Garante e le Procure, tuttavia, solo dall'esperienza concreta sarà possibile esprimere una valutazione sulla sua effettività, giacché la normativa sul punto non è, come si è visto, esaustiva.

Rimane anche aperta la questione afferente la possibilità della duplicazione delle sanzioni e quindi, sul rispetto del divieto di *ne bis in idem,* poiché, come si è visto, non si ravvisa nella disciplina alcun sistema che permetta di evitare il cumulo sanzionatorio e

[109] Ad avviso della menzionata dottrina, in realtà si potrebbe fare anche riferimento all'art. 2 par. 2 del Regolamento ove si specifica che lo stesso non si applica ai trattamenti di dati effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse e che secondo lo stesso art. 2 Codice Privacy: "il presente codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del regolamento"; tuttavia, secondo gli Autori, è altrettanto indicativo che non vi sia alcuna specifica disposizione che impedisca l'applicazione delle disposizioni ai trattamenti effettuati in ambito giudiziario. V. MANES, F. MAZZACUVA, cit., p. 179, in nota 40.

[110] E' il caso, riportato dall'Autore, del trattamento illecito di dati sensibili da parte della Autorità potrà integrare sia l'art. 43 comma 2 del decreto quanto l'art. 167, comma 2 del Codice Privacy; così, V. MANES, F. MAZZACUVA cit., p. 179 secondo cui la prevalenza di una fattispecie sull'altra dipenderà da valutazioni in termini di specialità reciproca o bilaterale.

sul quale non rimane che attendere le posizioni della giurisprudenza in fase di applicazione della disciplina.

Diritto all'oblio e dovere di provvedere delle pubbliche amministrazioni

DI GHERARDO CARULLO *

SOMMARIO: 1. Introduzione – 2. Liceità del trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e posizione giuridica dell'interessato – 3. Il diritto alla cancellazione dei dati personali e la conservazione dei dati in vista di un interesse pubblico o per l'esercizio di pubblici poteri – 4. Il dovere di provvedere sulla domanda di cancellazione di dati personali.

1. Introduzione

In ragione delle recenti novelle che hanno introdotto una nozione particolarmente ampia di trasparenza[1], comportante di sovente la pubblicazione *online* di dati personali[2], in questa sede si vuole approfondire in che termini il diritto alla cancellazione dei dati personali (c.d. diritto all'oblio[3]), come da ultimo disciplinato dall'art. 17 del Regolamento 2016/679/UE (Regolamento)[4], si atteggi nei confronti delle pubbliche amministrazioni ogniqualvolta le stesse si trovino a «trattare»[5] «dati personali»[6] per l'esecuzione delle proprie funzioni[7].

* Ricercatore (lett. b) nell'Università degli Studi di Milano, abilitato allo svolgimento delle funzioni di Professore di II fascia di Diritto Amministrativo, Dottore di ricerca in Diritto Amministrativo nella medesima Università, LLM al King's College di Londra.

[1] Intesa quale «accessibilità totale», ex art. 11, d.lgs. 150/ 2009, sul che si rinvia per tutti a D.U. GALETTA, *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, in *Federalismi.it*, 5, 2016, par. 4.

[2] In relazione ai possibili conflitti tra oneri di pubblicazione e tutela dei dati personali si veda l'analisi critica di G. GARDINI, *Il codice della trasparenza: Un primo passo verso il diritto all'informazione amministrativa?*, in *Giornale Dir. Amm.*, 8–9, 2014, par. 5. Sui profili di bilanciamento degli interessi nell'accesso civico generalizzato, D.U. GALETTA, *Accesso (civico) generalizzato ed esigenze di tutela dei dati personali ad un anno dall'entrata in vigore del Decreto FOIA: la trasparenza de "le vite degli altri"?*, in *federalismi.it*, 10, 2018.

[3] Sulla differenza di contenuto e correlazione tra «diritto alla cancellazione» ed «diritto all'oblio», cfr. D. BARBIERATO, *Osservazioni sul diritto all'oblio e la (mancata) novità del Regolamento UE 2016/679 sulla protezione dei dati personali*, in *Resp. civ. e prev.*, 6, 2017, par. 1.

[4] Sull'evoluzione di tale istituto nel diritto europeo cfr. per tutti F. ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679*, in *EuroJus.it*, 5, 2018, p. 18 e s.; sulle novità più rilevanti introdotte dal Regolamento, v. per tutti M. BOTTINO, *Approvato il nuovo regolamento generale per la protezione dei dati personali nell'UE*, in *EuroJus.it*, 4, 2016.

[5] V. la definizione *ex* art. 4, par. 1, n. 2.

[6] V. la definizione *ex* art. 4, par. 1, n. 1.

[7] Queste ultime intese quali momento di esercizio dei «propri poteri pubblicistici, idonei ad innovare nell'assetto preesistente dei rapporti giuridici», cfr. per tutti G. GRECO, *Introduzione*, in *Argomenti di diritto amministrativo*, vol. I, III Ed., Milano, 2017, p. 4.

Quanto alla preliminare questione di fondo circa l'applicabilità stessa del Regolamento a fattispecie in cui vengono in rilievo poteri autoritativi, si può anzitutto richiamare la definizione di «titolare del trattamento». Tra i soggetti che possono integrare tale nozione viene pacificamente inclusa «l'autorità pubblica», senza alcuna precisazione od esclusione in ordine al tipo di attività svolta[8]. Quanto all'applicabilità del Regolamento a fattispecie in cui il trattamento dei dati personali sia effettuato in ragione dell'esercizio di poteri autoritativi, può farsi riferimento all'art. 6, para. 1, lett. e), ai sensi del quale il trattamento è lecito laddove, tra gli altri, lo stesso sia «necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento». Sul punto occorre precisare che, come chiarito dal decimo considerando, è riconosciuta in tali casi agli Stati membri la facoltà «di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del [Regolamento]». Sicché, nel confermare che il Regolamento si applica anche ai casi in cui il trattamento dei dati sia eseguito in vista dell'esercizio di un potere autoritativo[9], si dovrà verificare se e quali norme speciali sussistano in relazione alla fattispecie esaminata.

Dato dunque per scontato che il bene della vita oggetto di tutela da parte del Regolamento siano i dati personali e la relativa capacità dispositiva da parte del titolare degli stessi[10], occorre valutare se, ed in che misura, l'interessato possa far valere la previsione di cui all'art. 17, para. 1, nei casi in cui il trattamento di dati personali sia effettuato sulla base dell'art. 6, para. 1, lett. e), del Regolamento.

---

[8] V. art. 4, par. 1, n. 7, Regolamento.

[9] In dottrina si è infatti sottolineato che, in aggiunta alle norme speciali dettate per i soggetti pubblici, a questi ultimi «rimangono applicabili tutti quegli obblighi generali cui sono assoggettati i titolari di trattamento privati», così S. D'ANCONA, *Trattamento e scambio di dati e documenti tra pubbliche amministrazioni, utilizzo delle nuove tecnologie e tutela della riservatezza tra diritto nazionale e diritto europeo*, in *Riv. it. dir. pubbl. com.*, 3, 2018, par. 4.

[10] Sul punto sin dal primo considerando del Regolamento viene chiarito che «la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale». Sulla qualificabilità della tutela dei dati personali quale diritto fondamentale, cfr. F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal Safe Harbour al Privacy Shield)*, in *Riv. dir. internaz.*, 3, 2016, *passim* e, dello stesso autore, *Alcune riflessioni a margine della nuova disciplina*, cit., p. 4 e ss.; B. NASCIMBENE, I. ANRÒ, *La tutela dei diritti fondamentali nella giurisprudenza della Corte di Giustizia: nuove sfide, nuove prospettive*, in *Riv. it. dir. pubbl. com.*, 2, 2017, par. 5.b. Sul rapporto tra tutela dei dati personali e diritto alla riservatezza non si registra invece unanimità di vedute, si veda ad esempio F. BALDUCCI ROMANO, *La Protezione dei Dati Personali nell'Unione Europea tra Libertà di Circolazione e Diritti Fondamentali dell'Uomo*, in *Riv. it. dir. pubbl. com.*, 6, 2015, par. 4, secondo la cui lettura la tutela dei dati personali, a differenza del diritto alla riservatezza, «non protegge la segretezza della persona, evitando la rappresentazione esterna indesiderata, bensì tutela l'identità dell'individuo nel caso di raccolta di informazioni sulla sua persona, consentendogli di disporre dei dati che lo riguardano, a prescindere dalla natura privata o meno di essi». Sulle interazioni tra tutela dei dati personali e diritto alla riservatezza cfr. anche COCUCCIO, *Il diritto all'oblio fra tutela della riservatezza e diritto all'informazione*, in *Dir. Famiglia*, 2, 2015, *passim*.

2. Liceità del trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e posizione giuridica dell'interessato

Ai sensi dell'art. 6 del Regolamento, il trattamento di dati personali è lecito solo «nella misura in cui»[11] ricorra una delle tassative condizioni dettate dalla norma stessa. Sul punto si è già in altra sede sottolineato che nei rapporti con le pubbliche amministrazioni se pur talvolta il consenso è effettivamente frutto di una libera scelta[12], altre volte lo stesso è un atto a vario modo non necessario. Dando dunque per acquisito quanto già più diffusamente esposto sul punto[13], in questa sede appare sufficiente concentrare l'analisi sulla già citata previsione di cui all'art. 6, para. 1, lett. e), del Regolamento[14].

In relazione a tale specifica condizione di liceità l'art. 6, para. 3, del Regolamento prescrive che il trattamento debba avvenire in forza di una base giuridica stabilita «dal diritto dell'Unione», ovvero «dal diritto dello Stato membro cui è soggetto il titolare del trattamento». In tal caso la medesima norma richiede espressamente che la finalità del trattamento sia necessaria in vista del pubblico interesse od il pubblico potere in forza del quale il trattamento stesso viene eseguito[15].

[11] Così letteralmente il primo periodo dell'articolo 6, paragrafo 1.

[12] Anche nel settore pubblico può infatti certamente trovare applicazione la prima condizione di liceità del trattamento, ai sensi della quale lo stesso è consentito se «l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità», articolo 6, paragrafo 1, lettera a) Regolamento 679/2016/UE.

[13] Si fa riferimento a quanto già esposto in G. CARULLO, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Torino, 2017, p. 48 e ss., ed in G. CARULLO, *Big Data e pubblica amministrazione nell'era delle banche dati interconnesse*, in *Conc. Merc.*, vol. 23, 2016, p. 191.

[14] Sono riconducibili a tale condizione di liceità quelle fattispecie in relazione alle quali il trattamento di dati personali è ad esempio strettamente necessario per lo svolgimento di una determinata funzione pubblica che ne giustifica la raccolta coattiva. In tali casi il soggetto interessato è spogliato della possibilità di autodeterminarsi in ordine al rilascio del consenso. Sul metodo di acquisizione delle informazioni nel settore pubblico cfr. anche E. SCHMIDT-AßMANN, *Relazione conclusiva*, in G. DELLA CANANEA, D.U. GALETTA, H.C.H. HOFMANN, J.-P. SCHNEIDER, J. ZILLER (a cura di), *Codice ReNEUAL del procedimento amministrativo dell'Unione Europea*, Napoli, 2016, p. XXXV; G. PASTORI, *Principi costituzionali sull'amministrazione e principio inquisitorio nel procedimento*, in M. CAMMELLI, M.P. GUERRA (a cura di), *Informazione e funzione amministrativa*, Bologna, 1997, p. 19; E. CARLONI, *Le verità amministrative: l'attività conoscitiva pubblica tra procedimento e processo*, Milano, 2011, p. 155; M. ANTONIOLI, *Riflessioni in tema di procedimento nel diritto anti-trust*, in *Riv. it. dir. pubbl. com.*, 1, 2000, p. 73.

[15] Cfr. art. 6, para. 3, Regolamento. In proposito già da tempo si era sostenuto in dottrina, in base alla precedente disciplina, che «in relazione ai soggetti pubblici la predeterminazione delle finalità del trattamento passa attraverso la lettura delle norme che attribuiscono agli stessi funzioni e competenze», v. C. MUCIO, *Il diritto alla riservatezza nella pubblica amministrazione: dati sensibili, dati personali e diritto di accesso*, Milano, 2003, p. 45. Pur se l'Autore avverte altresì che la sola norma non è di regola sufficiente, dovendo la stessa essere poi specificata per l'identificazione dei fini sottesi di volta in volta al trattamento.

Il legislatore nazionale ha in proposito previsto che «la base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento […] è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento»[16]. Tralasciando per il momento i singoli casi in cui la legge prevede in concreto la possibilità per l'amministrazione di trattare dati personali, ciò che preme in questa sede rilevare è che in tal modo viene a configurarsi un potere di tipo autoritativo, in quanto idoneo ad «incidere unilateralmente nella sfera giuridica altrui»[17]. Il soggetto – pubblico o privato[18] – a ciò autorizzato dalla legge in vista di un interesse pubblico, ovvero nell'esercizio di un pubblico potere, può trattare dati personali indipendentemente dal consenso dell'interessato. In altre parole, sulla base di tale disposizione l'amministrazione, nell'esercizio dei propri poteri autoritativi, può procedere al trattamento di dati personali anche indipendentemente dall'eventuale diverso volere del soggetto interessato e, per converso, in capo a quest'ultimo, non residua alcun margine di apprezzamento circa il rilascio del consenso, in quanto non richiesto.

3. Il diritto alla cancellazione dei dati personali e la conservazione dei dati in vista di un interesse pubblico o per l'esercizio di pubblici poteri

Rinviando alla dottrina che già si è occupata di inquadrare i caratteri essenziali del diritto all'oblio[19], per quanto qui interessa è sufficiente ricordare che ai sensi dell'art. 17,

[16] Art. 2-*ter*, d.lgs. 196/2003. Sul significato di legge e regolamento ai fini della norma, si veda S. D'ANCONA, *Trattamento e scambio di dati e documenti tra pubbliche amministrazioni*, cit., par. 5, e dottrina ivi citata, il quale spiega che «l'unico limite è che le previsioni di legge siano specifiche individuando puntualmente le principali caratteristiche dell'attività di comunicazione e non permettano in maniera del tutto generica lo scambio di dati personali».

[17] Secondo l'impostazione del potere autoritativo largamente condivisa in dottrina, su cui per tutti G. GRECO, M. CAFAGNO, *Attività amministrativa, provvedimenti e altri atti a regime amministrativo*, in *Argomenti di diritto amministrativo*, vol. I, III Ed., Milano, 2017, p. 164.

[18] La formale veste di ente di diritto privato a tal riguardo non pare poter determinare diverse considerazioni, posto che, ove una norma consenta il trattamento per tali ragioni, il soggetto che venga investito di tale potere, in forza dell'art. 1, c. 1-*ter*, l. 241/1990 dovrà comunque assicurare l'applicazione dei «principi di cui al comma 1» del medesimo articolo.

[19] Nonostante la recente codificazione, si tratta di istituto «di risalente tradizione (nato nella dottrina e nella giurisprudenza francese ha avuto un cammino parallelo al diritto della privacy)», G. AGRIFOGLIO, *Risarcimento e quantificazione del danno da lesione della privacy: dal danno alla persona al danno alla personalità*, in *Eur. dir. pr.*, 4, 2017, par. 5. Tra i numerosi contributi sul tema, tra i più recenti, sulle questioni legate all'uso dei dati nel settore pubblico: S. D'ANCONA, *Trattamento e scambio di dati e documenti tra pubbliche amministrazioni*, cit.; per le interazioni con libertà di espressione e reputazione: F. BARRA CARACCIOLO, *La tutela della personalità in internet*, in *Dir. informaz.*, 2, 2018; sulla procedimentalizzazione delle attività volte al trattamento di dati personali: A. IULIANI, *Note minime in tema di trattamento dei dati personali*, in *Eur. dir. pr.*, 1, 2018; sui profili risarcitori: G. AGRIFOGLIO, *Risarcimento e quantificazione del danno da lesione della privacy*, cit., problema peraltro già da tempo affrontato anche nei confronti delle pubbliche amministrazioni da G.P. CIRILLO, *Trattamento pubblico dei dati personali e responsabilità civile della P.A.*, in *Foro amm.*, 11–12, 1999; sul bilanciamento dei diversi interessi sottesi al diritto all'oblio: S. MARTINELLI, *Diritto all'oblio e motori di ricerca:*

para. 1, del Regolamento, al ricorrere di determinate condizioni, «l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali». Il terzo paragrafo del medesimo articolo 17 stabilisce tuttavia alcune eccezioni al ricorrere delle quali è sancito che entrambi i suddetti paragrafi «non si applicano».

È in particolare previsto che il diritto all'oblio non si applichi laddove il trattamento sia necessario per il perseguimento di un interesse pubblico o l'esercizio di un pubblico potere[20]. Ne deriva che ogniqualvolta il trattamento si fondi sulla condizione di liceità ex art. 6, para. 1, lett. e), sussistendo tale presupposto, l'amministrazione potrebbe opporre ad una domanda di cancellazione la sussistenza di una causa di esclusione ex art. 17, para. 3, fondata sui medesimi elementi che rendono lecito il trattamento.

Si potrebbe perciò ipotizzare che, in tali casi, non sia rinvenibile in capo all'interessato una posizione giuridica soggettiva oggetto di specifica tutela. Si potrebbe infatti immaginare che, in ragione della non applicabilità *tout court* della previsione di cui all'art. 17, para. 1, il soggetto interessato non abbia nulla a che pretendere rispetto al trattamento dei dati in sé considerato, potendo solo eventualmente lamentare l'illegittimo esercizio del potere in vista del quale tale trattamento è stato condotto.

Senonché il successivo articolo 21 del Regolamento disciplina il diritto di opposizione, pure richiamato dall'art. 17, para. 1, lett. c). Nei casi in cui il trattamento sia basato sulla condizione di legittimità di cui all'articolo 6, para. 1, lett. e)[21], l'articolo 21 prevede che l'interessato «in qualsiasi momento, per motivi connessi alla sua situazione particolare», possa pretendere che il titolare del trattamento si astenga dal trattare ulteriormente i propri dati personali, «salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria».

L'interessato può dunque opporsi al trattamento indipendentemente dall'attività svolta dal titolare dello stesso con i suoi dati, ossia, indipendentemente dagli eventuali atti adottati a valle del trattamento. Per altro verso la norma è particolarmente interessante laddove richiede che l'autorità, nel caso non ritenga di dare seguito all'opposizione, è

il bilanciamento tra memoria e oblio in Internet e le problematiche poste dalla de-indicizzazione, in *Dir. informaz.*, 3, 2017.

[20] Art. 17, para. 3, lett. b), Regolamento.

[21] Per completezza giova ricordare che la norma ammette l'opposizione anche nei casi di trattamento ai sensi dell'articolo 6, para. 1, lett. f), condizione di liceità che tuttavia non è applicabile alle «*autorità pubbliche nell'esecuzione dei loro compiti*» (articolo 6, para. 1, secondo periodo). Tralasciando in questa sede l'analisi dei rapporti di matrice esclusivamente privatistica, al riguardo pare sufficiente aggiungere che in relazione a tali fattispecie sembrerebbe particolarmente calzante l'idea proposta da G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2, 2000, p. 329, secondo il quale si avrebbe un «*interesse legittimo di diritto privato*».

tenuta a motivare il diniego, adducendo peraltro precisi motivi in grado di superare l'interesse fatto valere dall'interessato[22].

Ciò è particolarmente rilevante in quanto, laddove l'amministrazione non sia in grado di motivare congruamente un eventuale diniego, ovvero naturalmente nei casi in cui dia seguito alla richiesta, l'interessato ha diritto di ottenere (anche) la cancellazione dei dati. Ai sensi dell'articolo 17, para. 1, lett. c), l'interessato ha infatti diritto di ottenere l'eliminazione dei suoi dati se, a seguito di opposizione *ex* art. 21, «non sussiste alcun motivo legittimo prevalente per procedere al trattamento».

Da tale quadro se ne deve dunque dedurre che l'interessato può procedere nei confronti dell'amministrazione, onde esigere la cessazione del trattamento e l'eventuale cancellazione dei dati, anche indipendentemente dall'adozione di atti lesivi adottati a valle del trattamento stesso.

Tale lettura appare confermata anche dall'articolo 79 del Regolamento, rubricato «diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento». La norma dispone che «ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del […] regolamento siano stati violati a seguito di un trattamento».

Sul punto il nostro legislatore ha previsto che «tutte le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli articoli 78 e 79 del Regolamento e quelli comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali […] sono attribuite all'autorità giudiziaria ordinaria»[23].

Anche in ragione della particolare rilevanza dei diritti in gioco[24], si può perciò ritenere che l'interessato possa in tal sede far valere anche un'asserita erronea applicazione delle esclusioni di cui al paragrafo terzo summenzionato, ovvero l'incongruità della motivazione del diniego alla richiesta di opposizione. Se così non fosse, al titolare del trattamento basterebbe opporre una qualsiasi delle circostanze di cui all'art. 17, para. 3, ovvero una qualsiasi generica motivazione ai sensi dell'art. 21, per sottrarsi a qualsivoglia scrutinio circa la sussistenza, o meno, dei relativi presupposti. In tale situazione l'interessato non avrebbe modo di ricorrere ad un'autorità giudiziaria, se non attendendo l'eventuale emissione di un successivo provvedimento di cui lamentare l'illegittimità. Senonché, alla luce del tenore letterale dell'art. 79 del Regolamento e del

[22] Si è infatti commentato che «i dati personali, infatti, rappresentano una componente essenziale dell'identità di ciascun individuo che va preservata con ogni mezzo, ma, aggiungo, entro alcuni precisi confini, così che l'interesse privato e l'interesse pubblico possano pacificamente convivere», F. ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina*, cit., p. 2.
[23] Art. 152, d.lgs. 196/2003.
[24] Si è infatti sottolineato come «la protezione della riservatezza sia oggetto di un controllo ben più stringente rispetto alla protezione della libertà di espressione e di informazione, per quanto tali diritti siano tutti costituzionalizzati nella Carta dei diritti fondamentali dell'Unione europea», J. ALBERTI, *Damnatio memoriae e diritto all'oblio: i primi risvolti della sentenza Google Spain nei provvedimenti del Garante italiano per la protezione dei dati personali*, in *EuroJus.it*, 1, 2015, p. 3.

principio di effettività del diritto dell'Unione europea[25], tale lettura deve essere esclusa in quanto precluderebbe all'interessato l'accesso ad un rimedio «giurisdizionale effettivo».

All'interessato deve invece essere riconosciuto un diritto di azione innanzi all'autorità giudiziaria sia per sindacare la sussistenza dei presupposti stessi del trattamento, sia eventualmente per contestare un diniego ai sensi dell'art. 17, para. 3, ovvero la motivazione di cui all'art. 21, laddove reputi che il rifiuto dell'amministrazione non sia effettivamente giustificato.

Senonché la necessaria sussistenza di un interesse pubblico al trattamento dei dati sulla base della condizione di liceità del trattamento di cui all'art. 6, para. 1, lett. e), e la sostanziale coincidenza rispetto a tale presupposto della corrispondente eccezione prevista dall'art. 17, para. 3, potrebbe far ritenere che per l'amministrazione sia sufficiente opporre l'esistenza dei presupposti stessi che legittimano il trattamento.

Tale questione si risolve in sostanza in un problema di motivazione del diniego, che si atteggia in modo diverso a seconda della norma sulla base della quale viene disposto il trattamento stesso. La coincidenza o meno tra presupposti per il trattamento e motivi di diniego di una domanda di opposizione e/o di oblio appare dipendere dal carattere discrezionale, o meno, della valutazione che il titolare del trattamento è chiamato a svolgere in vista del trattamento. Si possono infatti avere casi in cui è configurabile un potere discrezionale, ove si debba valutare la persistenza di un interesse pubblico al trattamento rispetto all'interesse del privato alla cancellazione, come anche casi in cui tale ponderazione è a vario modo vincolata dal dettato legislativo[26]. Sicché, ogniqualvolta

[25] La Corte di giustizia ha in tal senso già affermato, in un caso relativo a delle domande di sovvenzioni, che «l'assenza di rimedi giurisdizionali contro una […] decisione di rigetto priva il richiedente del suo diritto a un ricorso effettivo», v. sentenza del 17 settembre 2014, nella causa C-562/12, *Liivimaa Lihaveis*, p. 71. Sull'affermazione nella giurisprudenza europea del diritto ad esperire un ricorso giurisdizionale innanzi a un giudice interno anche qualora esso non fosse espressamente previsto dal diritto nazionale, cfr. G. VITALE, *Il principio di effettività della tutela giurisdizionale nella Carta dei diritti fondamentali*, in *federalismi.it*, 5, 2018, p. 14. In dottrina si è altresì affermato che «la tutela giurisdizionale "piena ed effettiva" degli interessi protetti dalle norme non è altro che la proiezione soggettiva della piena ed effettiva attuazione delle norme stesse», così M. LIBERTINI, *Le nuove declinazioni del principio di effettività*, in *Eur. dir. pr.*, 4, 2018, par. 3.

[26] Si pensi, ad esempio, alla pubblicazione dei dati *ex* art. 14, c. 2, d.lgs. 33/2013. In tal caso è la norma stessa a prescrivere che i dati debbano essere soggetti a pubblicazione «per i tre anni successivi dalla cessazione del mandato o dell'incarico», sicché, prima di tale termine, non pare che residui in capo all'amministrazione alcun margine di apprezzamento circa la possibilità di accogliere un'eventuale domanda *ex* art. 17, para. 1. In altri casi lo scenario è invece opposto, come nel caso della liquidazione delle startup innovative, in relazione alle quali l'art. 31, c. 2, d.l. 179/2012, dispone che «decorsi dodici mesi dall'iscrizione nel Registro delle Imprese del decreto di apertura delle liquidazione [...], l'accesso ai dati relativi ai soci della stessa iscritti nel medesimo registro è consentito esclusivamente all'autorità giudiziaria e alle autorità di vigilanza», caso questo di «prevalenza dell'individuale "diritto all'oblio" sugli interessi generali protetti dal sistema di pubblicità legale», A. PICCHIONE, *Start up innovative e procedure di sovraindebitamento*, in *Riv. notariato*, 5, 2017, par. 5. In relazione ai dati contenuti nel Registro

con la domanda di cancellazione siano rappresentati all'amministrazione interessi nuovi o comunque diversi rispetto a quelli considerati in sede di trattamento dei dati, e la fonte normativa che legittima il trattamento lasci un qualche margine di apprezzamento in capo all'amministrazione, appare necessario che l'amministrazione conduca una nuova ponderazione degli stessi onde valutare la permanenza dei presupposti per il trattamento, ovvero per dare seguito alla domanda di cancellazione.

4. Il dovere di provvedere sulla domanda di cancellazione di dati personali

In base alla suesposta ricostruzione, nel caso in cui i dati siano trattati in base all'art. 6, para. 1, lett. e), all'interessato viene riconosciuta la possibilità di opporsi al trattamento e di avanzare un'istanza di cancellazione, mentre al titolare del trattamento spetta il compito di ponderare tale richiesta rispetto, rispettivamente, all'interesse al trattamento dei dati ed alle eccezioni di cui all'art. 17, para. 3, del Regolamento stesso e, in base a tale bilanciamento, accogliere o meno la domanda.

Come si è detto, nell'ambito del diritto all'oblio «il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali» a seguito della richiesta dell'interessato. Si deve perciò ritenere che anche l'avvio del procedimento di verifica dei presupposti per l'accoglimento, o meno, della domanda dell'interessato costituisca un obbligo per il titolare del trattamento, nella misura in cui tale verifica sia funzionale al rigetto della richiesta. In altri termini, laddove il titolare del trattamento non intenda accogliere l'istanza del privato, onde non rendersi inadempiente rispetto a tale obbligo dovrà, «senza ingiustificato ritardo», accertare che ricorra un giustificato motivo su cui fondare l'eventuale rifiuto.

Sicché, ai sensi dell'art. 2, c. 1, della l. 241/1990, si può ritenere che in tali casi il procedimento di verifica dei presupposti per la cancellazione dei dati «consegua obbligatoriamente» all'istanza di cancellazione e, perciò, l'amministrazione sia tenuta a «concluderlo mediante l'adozione di un provvedimento espresso». A fronte di una richiesta ai sensi dell'art. 17, para. 1, o 21 del Regolamento in relazione ad un trattamento eseguito sulla base dell'art. 6, para. 1, lett. e), si può quindi affermare che sorga un dovere di provvedere in capo al titolare del trattamento[27].

---

delle imprese, e sul relativo bilanciamento di interessi, si veda in particolare la sentenza della Corte di giustizia, 9 marzo 2017, nella causa C-398/15, *Manni*.

[27] Inteso questo alla luce del citato art. 2, c. 1, l. 241/1990, quale necessaria «produzione di un'attività che conduca ad un atto esplicito, motivato, rispondente all'iniziativa del procedimento, avente segno alternativo – positivo o negativo –, e che, almeno, impegni l'amministrazione a spendere la valutazione sufficiente ad emettere un atto di pregiudiziale "rifiuto di provvedimento", concernente i presupposti dell'inizio doveroso del procedimento», così A. CIOFFI, *Dovere di provvedere e pubblica amministrazione*, Milano, 2005, p. 106. Inteso quale dovere di «emettere un provvedimento che curi concretamente l'interesse pubblico», F. GOGGIAMANI, *La doverosità della pubblica amministrazione*, Torino, 2005, p. 109. Sul tema si rinvia per tutti a G. MARI, *L'obbligo di provvedere e i rimedi preventivi e successivi alla relativa violazione*, in M.A. SANDULLI (a cura di), *Princìpi e regole dell'azione amministrativa*, II Ed., Milano, 2017, *passim*.

Oltre che nei casi di diniego motivato, all'interessato è di conseguenza riconosciuto un diritto di azione anche nei casi in cui l'amministrazione non abbia provveduto, nei modi suddetti, entro il termine prescritto per la conclusione del procedimento[28].

Come si è anticipato, la giurisdizione sulla relativa controversia è devoluta in ogni caso al giudice ordinario. Rinviando alla dottrina che già si è occupata di tale scelta in ordine al riparto di giurisdizione[29], per quanto qui interessa è sufficiente sottolineare che il rito applicabile è quello di cui all'art. 10 del d.lgs. 150/2011, ai sensi del cui decimo comma «la sentenza che definisce il giudizio […] può prescrivere le misure necessarie anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile dei dati, nonché il risarcimento del danno»[30]. In giurisprudenza e in dottrina si è sottolineato che al giudice è in tali casi affidato un potere di decidere nel merito la questione controversa senza «i limiti interni che vincolano normalmente la giurisdizione ordinaria nei confronti dell'amministrazione»[31]. In applicazione di tale disposizione si è infatti già assistito a pronunce che hanno ad esempio annullato un provvedimento del Garante per la protezione dei dati personali decidendo nel merito circa l'onere di cancellazione di dati personali[32].

---

[28] Termine la cui determinazione non pare poter essere disposta *ex ante* una volta per tutte, essendo richiesto un intervento «senza ingiustificato ritardo», ma che appare dover essere valutato caso per caso.

[29] Si veda la ferma posizione di R. VILLATA, *« Lunga marcia » della Cassazione verso la giurisdizione unica (« Dimenticando » l'art. 103 della Costituzione)?*, in *Dir. Proc. Amm.*, 1, 2013, p. 326 e ss., il quale, a fronte dell'attuale assetto costituzionale, rigetta la tesi «che vorrebbe riconosciuta, malgrado quanto si legge in detta pronuncia, la discrezionalità piena del legislatore di affidare al giudice ordinario controversie in tema di interessi legittimi». L'Autore critica perciò la posizione di apertura verso la sentenza di M. ESPOSITO, *La "naturale" capacità espansiva della giurisdizione ordinaria*, in *Giur. it.*, 12, 2011, *passim*. In senso contrario a VILLATA si pone invece A. CORPACI, *Note per un dibattito in tema di sindacato della Cassazione sulle sentenze del Consiglio di Stato*, in *Dir. Pubb.*, 1, 2013, *passim*, il quale afferma in particolare che «occorre prendere atto della relativa variabilità consentita dalle regole enunciate dalla Costituzione», *ivi*, p. 352.

[30] Sul potere del giudice ordinario di annullare provvedimenti amministrativi e decidere la controversia nel merito sulla base di tale previsione si veda M. ESPOSITO, *La "naturale" capacità espansiva*, cit., *passim*.

[31] Così A. TRAVI, *Lezioni di giustizia amministrativa*, XIII Ed., Giappichelli, Torino, 2019, p. 132, in relazione all'articolo 10 del d.lgs. 150/2011 come da ultimo sostituito dall'articolo 17, comma 1, del d.lgs. 101/2018. Sul tema dei limiti del giudice ordinario nei confronti della pubblica amministrazione, per tutti si rinvia alla ricostruzione dello stato dell'arte esposta da P. CERBO, *Giudice ordinario e "sostituzione" della pubblica amministrazione*, in *Riv. trim. dir. proc. civ.*, vol. 66, 3, 2012, *passim*. In giurisprudenza si è affermato che «alla predetta autorità giudiziaria [ordinaria, n.d.a.] è consentito, per effetto di conforme disposizione del legislatore ordinario, di conoscere di interessi legittimi, di conoscere ed eventualmente annullare un atto della P.A., di incidere conseguentemente sui rapporti sottostanti secondo le diverse tipologie di intervento giurisdizionale previste», Cass. civ., Sez. Unite, 14 aprile 2011, n. 8487; in termini Cass. civ., Sez. Unite, 26 ottobre 2017, n. 25455.

[32] Si veda ad esempio la sentenza del Tribunale Milano del 28 settembre 2016, relativa all'impugnazione del provvedimento n. 156 del 2016 del Garante per la protezione dei dati

Nei casi di silenzio dell'amministrazione, così come in quelli di diniego espresso, si potrà perciò adire il giudice non solo al fine di accertare l'inadempimento rispetto alla domanda di cui all'art. 17, para. 1, o 21 del Regolamento, ma anche onde ottenere – sussistendone i requisiti nel merito – la condanna della stessa ad un *facere* specifico, ossia l'interruzione del trattamento e la rimozione dei dati personali oggetto della domanda di cancellazione[33]. Il che, rispetto agli ordinari poteri del giudice ordinario nei confronti della pubblica amministrazione[34], rappresenta un particolare caso in cui viene introdotta un'azione di adempimento anche laddove residuino eventuali margini di apprezzamento discrezionale da parte dell'amministrazione[35].

personali. Con tale atto era stato rigettato un reclamo presentato dall'interessato a seguito del diniego da parte del titolare del trattamento di dare seguito ad una domanda di cancellazione. In tal caso il Tribunale ha annullato il provvedimento ed ha quindi ordinato la cancellazione dei link oggetto della richiesta di cancellazione.

[33] In tal senso v. anche F. MIDIRI, *Il diritto alla protezione dei dati personali. Regolazione e tutela*, Napoli, 2017, pp. 302–303, secondo cui «l'autorità giudiziaria ordinaria ha il potere di conoscere i rapporti giuridici e di tutelare le posizioni soggettive nel rapporto di trattamento dei dati personali - in una parola del diritto alla protezione dei dati personali».

[34] Cfr. A. TRAVI, *Lezioni di giustizia amministrativa*, XIII Ed., Torino, 2019, p. 132, il quale spiega che il rito in materia di protezione dei dati personali di cui all'articolo 10 del d.lgs. 150/2011 come da ultimo sostituito dall'articolo 17, comma 1, del d.lgs. 101/2018 supera «*i limiti interni che vincolano normalmente la giurisdizione ordinaria nei confronti dell'amministrazione*». Sul tema dei limiti del giudice ordinario nei confronti della pubblica amministrazione, per tutti si rinvia alla ricostruzione dello stato dell'arte esposta da P. CERBO, *Giudice ordinario e "sostituzione" della pubblica amministrazione*, in *Riv. trim. dir. proc. civ.*, vol. 66, 3, 2012, *passim*.

[35] Il che, senza voler entrare nel merito di quanto già affermato, parrebbe integrare un ulteriore esempio di «conflitto tra giurisdizioni» nei termini esposti da R. VILLATA, *'Lunga marcia' della Cassazione*, cit., p. 341 e ss..