Il trattamento dei dati personali in ambito giudiziario

Quaderno 5

Volume a cura di: Antonella Ciriello e Gianluca Grasso, *componenti del Comitato direttivo della Scuola superiore della magistratura,* e Doris Lo Moro, *Responsabile della protezione dei dati personali del Ministero della giustizia*

Contributo redazionale: Ilaria Laezza *nell'ambito del tirocinio curriculare presso la Scuola superiore della magistratura, a seguito della convenzione sottoscritta con la Libera Università Internazionale degli Studi Sociali Guido Carli*

Collana a cura del Comitato direttivo della Scuola superiore della magistratura:

Giorgio Lattanzi, Marco Maria Alma, Lorenza Calcagno, Antonella Ciriello, Claudio Consolo, Fabrizio Di Marzio, Costantino De Robbio, Gian Luigi Gatta, Gianluca Grasso, Sara Lembo, Marisaria Maugeri, Gabriele Positano

POLIGRAFICO E ZECCA DELLO STATO ITALIANO
IPZS S.p.A.

Coordinamento editoriale e cura del progetto grafico:

Camilla Pergoli Campanelli

ISBN 9791280600035

Il trattamento dei dati personali in ambito giudiziario

Quaderno 5

La Scuola e la collana dei Quaderni

La Magna carta dei giudici, adottata dal Consiglio consultivo dei giudici europei, facendo proprio un principio condiviso nell'ambito dei diversi ordinamenti europei, riconosce nella formazione "un importante elemento di garanzia dell'indipendenza dei giudici, nonché della qualità e dell'efficacia del sistema giudiziario" (pt. 8).

In questa prospettiva la Scuola superiore della magistratura raccoglie l'esperienza maturata dal Csm nell'attività di preparazione e aggiornamento professionale dei giudici e dei pubblici ministeri, che è proseguita fino all'entrata in funzione della Scuola, cui la riforma dell'ordinamento giudiziario ha affidato la competenza esclusiva in tema di formazione dei magistrati (d.lgs. n. 26 del 2006).

Il primo Comitato direttivo si è insediato il 24 novembre 2011. Il 15 ottobre 2012 è stato inaugurato il primo corso di formazione della Scuola dedicato ai magistrati ordinari in tirocinio e nel gennaio 2013 è stato avviato il primo programma di formazione permanente.

Oggi la Scuola è impegnata in tutti i settori della formazione dei magistrati: iniziale, permanente, decentrata, dirigenti, onorari, tirocinanti, internazionale.

Accanto all'organizzazione e alla realizzazione delle sessioni di aggiornamento professionale, la documentazione giuridica rappresenta un tema centrale nelle attività di formazione.

La Scuola mette già a disposizione di tutti i magistrati italiani una ricca biblioteca telematica all'interno della sezione del sito dedicata alle banche dati. Altrettanto fondamentale è il materiale didattico elaborato nel contesto delle sessioni formative e disponibile sul sito istituzionale, nell'ambito di ciascun corso.

La collana dei Quaderni, resa possibile grazie alla collaborazione con il Poligrafico e Zecca dello Stato italiano, nasce con l'intento di consentire la più ampia fruizione dei contributi più significativi di questo materiale di studio e dei risultati dell'attività di ricerca svolta dall'istituzione.

La collana si collega idealmente a quella inaugurata negli anni '80 del secolo scorso dal Csm e dedicata agli incontri di studio per i magistrati organizzati nell'ambito della formazione iniziale e continua, all'epoca di competenza consiliare.

I singoli volumi sono disponibili liberamente sul sito della Scuola e nell'ambito della biblioteca virtuale che contiene le pubblicazioni ufficiali dello Stato.

INDICE

Gli autori

Doris Lo Moro
Responsabile della protezione dei dati personali del Ministero della giustizia

Giusella Finocchiaro
Professoressa ordinaria di diritto di internet e di diritto privato nell'Università di Bologna

Federica Resta
Autorità Garante per la protezione dei dati personali

Filippo Donati
Componente del Consiglio superiore della magistratura

Giovanni Canzio
Primo presidente emerito della Corte di Cassazione

Francesco Caprioli
Professore ordinario di Diritto processuale penale Università degli Studi di Torino

Alessandro Centonze
Consigliere della Corte di Cassazione

Celestina Iannone
Direttrice della Direzione della Ricerca e Documentazione della Corte di Giustizia dell'Unione europea

Emma Salemme
Direzione della Ricerca e Documentazione della Corte di Giustizia dell'Unione europea

Edoardo Buonvino
Giudice del Tribunale di Roma

Martina Flamini
Giudice del tribunale di Milano

Monica Velletti
Presidente di sezione del Tribunale di Terni

Maria Cristina Amoroso
Magistrato addetto all'ufficio del Massimario e del ruolo della Corte di Cassazione

Federica Fiorillo
Magistrato addetto all'ufficio di Gabinetto del Ministro della Giustizia

Armando Spataro
già Procuratore della Repubblica presso il Tribunale di Torino

Presentazione

1. Il presente volume raccoglie i contributi del corso "Trattamento dei dati personali in ambito giudiziario" (P21003), tenutosi il 18 e 19 gennaio 2021, con modalità di formazione a distanza, stante il perdurare della crisi sanitaria derivante dall'epidemia Covid-19. Si tratta di una tematica fondamentale per le situazioni soggettive coinvolte nel contesto dell'esercizio dell'attività giudiziaria.

2. Il tema del trattamento dei dati personali è diventato negli ultimi anni ineludibile. Il "*diritto alla protezione dei dati di carattere personale*" ha fatto ingresso formale nel contesto europeo con l'articolo 8 della Carta dei diritti dell'Unione europea (Carta di Nizza), proclamata nel 2000 e diventata giuridicamente vincolante con la firma del Trattato di Lisbona, entrato in vigore nel 2009.

Ma già prima si discuteva da tempo di diritto alla *privacy* e nel nostro ordinamento il cd. diritto alla riservatezza trovava riferimenti nella stessa Carta Costituzionale che sancisce, in particolare, l'inviolabilità del domicilio (articolo 14) e la libertà e la segretezza della corrispondenza (articolo 15) e soprattutto riconosce e garantisce i diritti inviolabili della persona (articolo 2).

Non c'è dubbio comunque che il concetto e il valore della *privacy* si è fatto strada e si è imposto sul piano culturale, assumendo via via connotazioni sempre più ampie, a fronte di cambiamenti che mettevano – e mettono – a rischio informazioni e dati la cui diffusione può ledere la dignità delle persone e complicarne i rapporti sociali, ai quali in Italia, anche per l'impegno di singole personalità di particolare spessore, si è fatto fronte con il "*Codice in materia di protezione dei dati personali*", adottato con decreto legislativo n. 196 del 30 giugno 2003, più volte modificato.

Particolarmente fecondo, sul piano normativo, è stato il decennio appena conclusosi che ha visto emanare: a livello europeo, il Regolamento (UE) 2016/679 "*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*" (GDPR), direttamente applicabile a decorrere dal 25 maggio 2018 in tutti gli Stati membri, e la Direttiva (UE) 2016/680, in materia di "*trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali…*"; nel contesto nazionale, il decreto legislativo del 18 maggio n. 51, di attuazione della Direttiva UE 2016/680, e il decreto legislativo del 10 agosto 2018 n. 101 che contiene una serie di disposizioni per l'adeguamento della normativa nazionale al GDPR, che modificano in maniera significativa il Codice in materia di protezione dei dati personali; disegnando così un contesto normativo più completo e innovativo, con il quale ci si misura giornalmente anche nelle aule giudiziarie.

3. Il corso nasce con l'obiettivo ambizioso di approfondire il quadro normativo, al quale poco sopra si è solo accennato, e, al contempo, verificarne la ricaduta pratica in una serie di casi già sottoposti al vaglio del Garante privacy e/o dell'autorità giudiziaria o comunque ipotizzabili nel contenzioso in materia, cercando anche di cogliere buone pratiche ed elementi di riflessione per una migliore valutazione di casi ancora non del tutto definiti sul piano normativo.

La stessa scelta dei relatori ha rafforzato l'obiettivo, coinvolgendo personalità di diversa estrazione che hanno messo a disposizione competenze direttamente maturate sul campo, con una varietà di esperienze e un approccio che complessivamente si è dimostrato capace di coinvolgere i partecipanti al Corso che ha avuto momenti particolarmente vivaci.

La prima giornata è cominciata con gli interventi del Presidente del Comitato Direttivo della Scuola Superiore della Magistratura, Giorgio Lattanzi, e del Presidente del Garante per la protezione dati, Pasquale Stanzione, i quali sono andati oltre l'indirizzo di saluto, attestando piena convergenza sulla necessità di rafforzare il confronto e la collaborazione sulla protezione dei dati.

La mattinata del 18 gennaio è stata dedicata all'approfondimento normativo, al fine di garantire la conoscenza da parte dei partecipanti al Corso del contesto normativo di riferimento.

Alla prof. Giusella Finocchiaro, che è stata Presidente della Commissione istituita presso il Ministero della Giustizia per la predisposizione dei decreti legislativi di recepimento ed adeguamento dell'ordinamento interno alle prescrizioni europee in materia di protezione dei dati personali, è stata affidata la relazione sulla normativa europea ed italiana in materia di tutela dei dati personali ("*La tutela dei dati personali tra Regolamento UE 2016/679 e d.lgs. 101/2018*"). Con l'intervento di inquadramento della prof. Finocchiaro si sono acquisiti anche elementi di dettaglio sulla normativa e sulla scelta di intervenire con modifiche al Codice in materia di protezione dei dati personali, anziché con un autonomo testo, portata avanti con il decreto legislativo n. 101/2018.

Il compito di approfondire il trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali è stato affidato a Federica Resta, coordinatrice dell'Ufficio di Presidenza del Garante per la protezione dei dati personali e attualmente direttrice del Servizio Affari legislativi e istituzionali, che ha fatto parte del Gruppo di Lavoro chiamato a redigere lo schema di decreto legislativo di recepimento della Direttiva (UE) 680/2016. Con tale relazione ("*La tutela dei dati personali in ambito giudiziario e di polizia – direttiva UE 2016/680 e d.lgs. 51/2018*") sono state illustrate le caratteristiche del richiamato decreto legislativo e le tutele rimediali per i terzi i cui dati siano stati acquisiti nell'ambito del procedimento penali.

La sessione mattutina si è conclusa con la relazione su "*Minori – Aspetti specifici della protezione dati*" affidata a Federica Fiorillo, giudice, attualmente fuori ruolo presso l'ufficio di Gabinetto del Ministro della Giustizia (all'epoca della relazione già in servizio presso il Ministero della giustizia), che si è occupata di diritto di famiglia presso i Tribunali di Vicenza e Padova ed è Esperto indipendente del Consiglio di Europa nell'ambito del Comitato sui diritti e l'interesse superiore del fanciullo nella separazione parentale e nei procedimenti di affidamento. Con tale relazione, dopo una panoramica generale di diritto internazionale e diritto interno, sono state affrontate questioni inerenti alla tutela dei dati personali dei minori con particolare riferimento alla loro azione nel mondo digitale e nella rete.

Nel pomeriggio, si è discusso del "*Rapporto tra Garante Privacy e autorità giudiziaria*".

Ne ha parlato per prima, affrontando il tema della "*tutela civile della persona e dell'identità*", Martina Flamini, giudice presso il Tribunale di Milano, che è autrice di varie pubblicazioni sull'argomento e ha anche prodotto una serie di sentenze, per lo più da lei stessa redatte, su casi sottoposti alla valutazione del Tribunale di Milano. Nell'esaminare il tema, la relatrice si è soffermata sul rapporto tra procedimento amministrativo e procedimento giurisdizionale, con riguardo alla portata del principio di alternatività di cui all'art. 140-*bis* Codice in materia di protezione dei dati personali. Particolare attenzione è stata dedicata alla tutela della persona ed ai rimedi esperibili dinanzi al giudice, attraverso l'esame di fattispecie portate all'esame della giurisprudenza di merito. Nell'analisi dei casi presentati, ci si è soffermati sul rimedio della c.d. deindicizzazione globale (oggetto di pronunce differenti da parte del Garante privacy e del Tribunale di Milano) alla luce della posizione assunta dalla Corte di Giustizia.

A seguire, ha svolto la sua relazione Maria Cristina Amoroso, giudice addetto all'Ufficio del Massimario e del Ruolo presso la Corte di Cassazione, con pregressa esperienza di pubblico ministero, che ha affrontato il tema della "*tutela penale della persona e dell'identità*", offrendo alla discussione, con riferimento a singole fattispecie incriminatrici, una serie di spunti pratici che hanno comprovato l'importanza dell'approfondimento del tema della tutela della *privacy*, anche ai fini delle indagini e più in generale dei processi penali per reati coinvolgenti dati personali.

Nella stessa sessione pomeridiana, si è parlato di intelligenza artificiale.

Ne ha parlato per primo Giovanni Canzio, Primo Presidente Emerito della Corte Suprema di Cassazione, che da qualche tempo partecipa autorevolmente alla discussione sull'utilizzo dell'intelligenza artificiale nel sistema giustizia. Il relatore ha innanzitutto inquadrato il problema sul piano teorico, sottolineando,

con riferimento al nostro Paese, che "*la legge (art. 101, comma 2 Cost.) e la ragione (art. 111, comma 6 Cost.) costituiscono presidi della razionalità del giudicare e fonti di legittimazione della giurisdizione e dei giudici*". Con riferimento poi al fenomeno dell'utilizzo da parte di alcune Corti statunitensi di tecniche informatiche per misurare, in particolare, il rischio di recidiva, si è soffermato sulle critiche formulate dalla comunità dei giuristi con riguardo alle possibili distorsioni cognitive dell'algoritmo utilizzato (che potrebbe essere, per esempio, fondato su dati discriminatori o opachi) e sulla necessità che "*la coerenza logica del calcolo algoritmico va verificata in un processo d'integrazione fra le misure quantitative, ricche e imponenti, da esso offerte con il percorso cognitivo e decisorio del giudice*". L'utilizzo "*della tecnologia digitale, di software informatici e algoritmi predittivi … potrebbero certamente contribuire a restituire al funzionamento della giustizia penale una più adeguata immagine di efficacia e qualità*" ma la decisione competerebbe comunque al giudice e alla sua professionalità. E ciò in linea con la visione umanocentrica dell'Unione europea (Carta etica elaborata da Cepej e proposta di Regolamento sull'IA della Commissione europea) che giustifica l'opzione per "*lo standard 'debole' della intelligenza artificiale, che consenta all'uomo di mantenere comunque il controllo della macchina*".

A seguire è intervenuto sul tema dell'impatto dell'intelligenza artificiale nel processo civile Filippo Donati, docente universitario, attualmente componente del Consiglio Superiore della Magistratura, il quale, dopo aver sottolineato che, a livello europeo, esiste una radicata consapevolezza delle potenzialità che l'intelligenza artificiale offre per il settore giustizia, si è soffermato sulle grandi potenzialità e sui rischi da contrastare, sottolineando che comunque "*anche se gli ostacoli di natura tecnica venissero superati, rimarrebbero ostacoli di natura giuridica a certi tipo di utilizzo dell'IA nel campo della giustizia*", a cominciare dal fatto che la sostituzione di giudici con robot non è consentita dalla nostra Costituzione e che la previsione di forme obbligatorie di soluzione automatizzata violerebbe numerose disposizioni costituzionali. Il relatore si è poi soffermato su concrete ipotesi di possibili impieghi dell'IA (come per la quantificazione di importi monetari nell'ambito di giudizi civili o per i servizi di traduzione e di dettatura automatica), sottolineando che "*in definitiva, nuovi sistemi di IA, se utilizzati in modo tale da garantire il rispetto dei diritti fondamentali, potranno contribuire ad un miglioramento complessivo della qualità e dell'efficienza della nostra giustizia*".

La mattina della seconda giornata si è aperta con la relazione su "Intercettazioni e tutela della *privacy* nella cornice costituzionale" svolta dal prof. Francesco Caprioli, ordinario di procedura penale, anch'egli componente del gruppo di lavoro presieduto dalla Finocchiaro, che nella sua attività di ricerca ha approfon-

dito, in particolare, il tema del diritto alla segretezza delle comunicazioni (nei suoi rapporti con la disciplina della prova penale). Il relatore si è soffermato sull'incidenza delle attività di intercettazione su diritti fondamentali della persona quali il diritto alla segretezza della corrispondenza e delle altre forme di comunicazione e il diritto all'inviolabilità del domicilio e sulle condizioni che l'atto investigativo deve soddisfare per rispettare i precetti costituzionali. Ha poi trattato il tema dell'incidenza delle intercettazioni sulla riservatezza dei terzi coinvolti nei colloqui intercettati e delle persone a cui si fa eventualmente riferimento. Si è quindi soffermato sulle lesioni che si consumano con l'uso della notizia riservata nel processo o tramite la pubblicazione dell'atto processuale. Non sono mancati riferimenti ai problemi più attuali quali quelli riconducibili a strumenti particolarmente invasivi, come i captatori informatici, e quelli relativi al meccanismo di selezione delle intercettazioni rilevanti, introdotto nel recente passato, su cui però il legislatore è tornato indietro.

A seguire, si è passati ad un altro tema con implicazioni significative sulla valutazione delle prove, questa volta nel settore civile. Monica Velletti, attualmente Presidente della Sezione civile del Tribunale di Terni, che per anni si è occupata di diritto di famiglia come giudice del Tribunale di Roma, ha svolto la relazione su "*Diritto alla difesa e diritto alla privacy – Disciplina della prova nei procedimenti di diritto di famiglia*". La relatrice ha prima chiarito la cornice normativa interna ed internazionale per l'inquadramento della questione, passando poi ad affrontare il tema dell'utilizzo delle prove acquisite illecitamente nei procedimenti di diritto di famiglia, distinguendo tra la condotta finalizzata alla ricerca della prova, che potrebbe essere oggetto di accertamento e di sanzione penale, e la richiesta di utilizzo del documento illecitamente acquisito. Le conclusioni che ha offerto alla discussione, dopo aver esposto e approfondito le possibili soluzioni diverse e dopo aver richiamato sentenze della Corte di Cassazione sul tema del "*bilanciamento degli interessi*", sono state nel senso che "*nell'ambito dei procedimenti di diritto di famiglia il bilanciamento di interessi potrebbe far propendere per l'ammissibilità di prove illecitamente acquisite in ogni caso in cui la prova sia posta a fondamento di domande attinenti diritti fondamentali di rango elevato*". La relatrice ha quindi proceduto alla disamina di numerosi casi affrontati in sede giurisprudenziale, per evidenziare la mancanza di orientamenti univoci stante la presenza di pronunce a sostegno della "*tesi del bilanciamento di interessi*", prevalenti tra le decisioni di merito, ovvero della inammissibilità delle prove illecitamente acquisite.

Nella sessione mattutina del 19 gennaio si è poi svolta una importante tavola rotonda su "*Il regime di pubblicità dei provvedimenti giudiziari (l'anonimizzazione delle sentenze)*" a cui hanno partecipato, con la scrivente, che è stata

Esperto formatore del corso, Celestina Iannone, Direttrice della direzione della ricerca e della documentazione della Corte di Giustizia, Federica Resta, dirigente dell'Autorità Garante (in sostituzione di Fabio Mattei, Segretario Generale della stessa Autorità), Pietro Lupi, magistrato della Direzione Generale dei sistemi informativi automatizzati del Ministero della Giustizia, e Giovanni Rocchi, avvocato.

L'occasione è servita per fare il punto sulle pratiche, non omogenee, seguite rispettivamente: a livello europeo, dalla Corte di Giustizia, che da tempo ha previsto la sostituzione con iniziali, in tutti i documenti pubblicati, dei nomi delle persone fisiche coinvolte nelle cause; e a livello nazionale, dalla Corte Costituzionale, che come tale non è soggetta alle disposizioni del Codice in materia di protezione dei dati personali ma tiene comunque conto delle normativa prevedendo l'oscuramento dei dati contenuti nelle sue pronunce, che nascono e circolano con i nomi dei soggetti coinvolti siglati (procedura di oscuramento che nell'ultimo biennio ha riguardato la totalità dei processi penali e gran parte degli altri procedimenti), nonché dalle supreme magistrature nazionali (Corte di Cassazione e Consiglio di Stato) che seguono proprie articolate procedure nel rispetto dell'articolo 52 del Codice in materia di protezione dei dati personali, prevedendo che, nei casi di anonimizzazione, si provveda *ex post* previa annotazione sul l'originale integro.

La discussione si è poi concentrata sul citato articolo 52, che prevede l'anonimizzazione su richiesta e/o d'ufficio e i casi di anonimizzazione obbligatoria, sulla necessità che l' interpretazione della norma tenga conto dei principi introdotti dal Regolamento (UE) 2016/679, sull'estensione pretoria dei casi di oscuramento obbligatorio, sulla portata del potere di oscuramento d'ufficio che potrebbe essere utilizzato con maggiore ampiezza anche in considerazione del pregiudizio che deriva agli interessati dalla reperibilità in rete dei loro dati, sull'opportunità sempre più avvertita di prevedere la deindicizzazione dei provvedimenti giudiziari, anche a legislazione invariata, sulla necessità che il bilanciamento degli interessi non contragga oltre il necessario il diritto alla difesa e alla circolazione delle informazioni. Sono state inoltre acquisite informazioni su progetti avviati dal Ministero della Giustizia finalizzati a rafforzare gli strumenti di informatica giuridica garantendo la normativa in materia di protezione dati.

Nella sessione pomeridiana sono stati organizzati quattro gruppi di lavoro.

Nel primo gruppo (civile), coordinato da Carmelo Barbieri, giudice del Tribunale civile di Milano e Consigliere giuridico del Vice Presidente del CSM, si è trattato il tema "*Intelligenza artificiale e processo civile – Possibili aspetti pratici*". L'occasione è servita per verificare sulla base di ipotesi concrete, alcune delle quali anche normate, rischi ma anche opportunità dell'applicazione di strumenti di intelligenza artificiale, concentrandosi non tanto e non solo sulle piattaforme di giustizia predittiva, già presenti nel panorama comparatistico, ma, soprattutto,

sugli strumenti di IA funzionali alla disamina degli elementi istruttori versati in sede processuale, in grado di ridurre i più comuni *bias* connessi alla decisione umana. In una chiave, dunque, di supporto e non di sostituzione dello *ius dicere*.

Nel secondo gruppo (penale), coordinato da Armando Spataro, già Procuratore della Repubblica presso il Tribunale di Torino, si è trattato il tema "*Il dovere di riservatezza nell'attività giudiziari*". La discussione, di grande attualità, si è svolta partendo dalle "Direttive per i magistrati dell'Ufficio, con particolare riferimento ai rapporti con la Polizia Giudiziaria" emanate nell'ottobre 2018 dal Coordinatore, all'epoca in servizio. Ci si è poi confrontati, in particolare, su alcune prassi seguite soprattutto da Uffici di Procura e sulla necessità di una riflessione comune su informazione e giustizia tra magistrati, avvocati e giornalisti.

Nel terzo gruppo (civile), coordinato da Edoardo Buonvino, giudice del Tribunale di Roma, si è trattato il tema "*Il dato personale nei provvedimenti in materia civile, contenziosa e di volontaria giurisdizione. Circolazione dei provvedimenti ed esigenza di riservatezza delle persone cui essi si riferiscono*". La discussione si è così occupata anche di casi relativi alla materia della volontaria giurisdizione di competenza del giudice tutelare, con specifico riguardo ai profili concernenti gli adulti vulnerabili beneficiari di misure di protezione, spesso trascurati nel dibattito generale ma che in concreto, sotto il profilo della tutela dei dati personali, comportano problematiche che richiedono risposte immediate.

Nel quarto gruppo (penale), coordinato da Alessandro Centonze, Consigliere della Corte di Cassazione, si è trattato il tema "*La tutela dei dati personali e l'accesso alle informazioni sensibili nei provvedimenti della Cassazione*". Il coordinatore ha introdotto la discussione fornendo, in particolare, indicazioni dettagliate sulle procedure seguite dalla Cassazione a tutela dei dati personali, rispettivamente nel settore civile e in quello penale. A seguire, anche su sollecitazione dei partecipanti al Gruppo, si è passati all'esame di casi concreti.

La sessione si è conclusa in plenaria con una breve esposizione da parte di un rappresentante di ciascun gruppo delle questione emerse e del dibattito svolto.

Il corso è stato seguito con molto interesse e gli interventi dei relatori sono stati arricchiti dal dibattito che ha toccato anche aspetti non trattati nelle relazioni.

Il presente volume raccoglie le relazioni scritte depositate da gran parte dei relatori, per la cui pubblicazione non si è seguito l'ordine degli interventi, richiamato nella presentazione, ma si è invece tenuto conto dei profili sistematici. Mancano, oltre agli interventi svolti in sede di dibattito, gli interventi dei relatori che hanno contribuito alla riuscita del corso ma non hanno depositato una relazione scritta.

Doris Lo Moro

Giusella Finocchiaro

Il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*

Sommario: 1. Le ragioni alla base dell'emanazione del Regolamento. – 2. L'oggetto del Regolamento. – 3. Il titolo del Regolamento. – 4. Il duplice oggetto e la necessità del bilanciamento. – 5. Due visioni sottese. – 6. Il limite del Regolamento. – 7. Un sistema in costruzione. – 8. L'adeguamento della normativa italiana al Regolamento europeo

1. Le ragioni alla base dell'emanazione del Regolamento

Le ragioni che hanno condotto all'emanazione del Regolamento europeo 2016/679 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" sono molteplici[1].

---

* Il contributo riproduce il Commento all'articolo 1 del Regolamento (UE) 2016/679, pubblicato in *Codice della privacy e della data protection,* a cura di Oreste Pollicino, Giorgio Resta, Giusella Finocchiaro, Roberto D'Orazio, nella collana *Fonti del diritto italiano*, Milano, 2021.

[1] In dottrina: Alpa, *La disciplina dei dati personali*, Roma, 1998; Alpa, *La 'proprietà' dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, (a cura di) Zorzi, Milano, 2019, 11-34; Alpa-Resta, *Le persone fisiche e i diritti della personalità*, in *Trattato di diritto civile*, (diretto da) Sacco, Milano, 2019; Auletta, *Riservatezza e tutela della personalità*, Milano, 1978; Barba-Pagliantini (a cura di), *Delle persone. Vol. II*, in *Commentario del codice civile*, (diretto da) Gabrielli, Milano, 2019; Barbera, *La Carta europea dei diritti e la Costituzione italiana*, in *Le libertà e i diritti nella prospettiva europea. Atti della Giornata di studio in memoria di Paolo Barile (Firenze, 25 giugno 2001)*, Padova, 2002, 107-128; Bianca-Busnelli (a cura di), *La protezione dei dati personali. Commentario al D.lgs. 30 giugno 2003 n. 196 (codice della privacy)*, Padova, 2007; Bifulco-Cartabia-Celotto (a cura di), *L'Europa dei diritti. Commentario alla Carta dei diritti fondamentali dell'Unione europea*, Bologna, 2001; Bravo, *Le condizioni di liceità del trattamento di dati personali,* in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, (diretto da) Finocchiaro, Bologna, 2019, 110-193; Busnelli, *Nota introduttiva al commento della l. 31 dicembre 1996, n. 675. Spunti per un inquadramento sistematico*, in *Tutela della privacy. Commentario alla l. 675/96,* (a cura di) Bianca-Busnelli-Bellelli-Luiso-Navaretta-Patti-Vecchi, Padova, 1999,

228-233; Busnelli, *Le alternative sorti del principio di dignità della persona umana*, RDC, 5, 2019, 1071-1085; Califano-Colapietro (a cura di), *Innovazione, tecnologia e valore della persona. Il diritto alla protezione dei dati personali nel regolamento UE 2016/679*, Napoli, 2018; Cuffaro, *Quel che resta di un codice: il D.lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, CG, 2018, 10, 1181-1185; 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-D'Orazio-Ricciuto, Torino, 2019, 1-22, spec. 17 ss.; Cuffaro-D'Orazio-Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; Cuffaro-Ricciuto-Zeno Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998; D'Orazio, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in *I dati personali nel diritto europeo*, (a cura di) Cuffaro-D'Orazio-Ricciuto, Torino, 2019, 61-84; Finocchiaro, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, D INF, 3, 2012, 383-394; Finocchiaro, *Privacy e protezione dei dati personali, Disciplina e strumenti operativi*, Bologna, 2012; Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, D INF, 4-5, 2014, 591-604; Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali: da Google Spain a Schrems*, D INF, 4-5, 2015, 779-799; Finocchiaro (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; Finocchiaro, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali,* (diretto da) Finocchiaro, Bologna, 2017, 1-22; Finocchiaro (diretto da), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019; Finocchiaro, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, (diretto da) Finocchiaro, Bologna, 2019, 1-26; Gambaro, *Categorie del diritto privato e linguaggio delle carte dei diritti fondamentali*, in *I diritti fondamentali in Europa e il diritto privato*, (a cura di) Caggia-Resta, Roma, 2019, 43-64; Gutwirth-Leenes-De Hert (a cura di), *Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection*, Dordrecht, 2016; Hijmans, *The European Union as Guardian of Internet Privacy. The Story of Art. 16 TFEU*, Cham, 2016; Krotoszynski, *Privacy Revisited. A Global Perspective on the Right to Be Left Alone*, New York, 2016; Kuner-Bygrave-Docksey-Drechsler (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, 2019; Lipari, *Le categorie del diritto civile*, Milano, 2013, spec. 122-127; Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori,* C IMPR, 1, 2018, 106-125; Macario, *La protezione dei dati personali nel diritto europeo*, in *La disciplina del trattamento di dati personali*, (a cura di) Cuffaro-Ricciuto, Torino, 1997, 5-60; Messina, *L'adeguamento della normativa nazionale al Regolamento*, in *I dati personali nel diritto europeo*, (a cura di) Cuffaro-D'Orazio-Ricciuto, Torino, 2019, 119-160; Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice* privacy*)*, Milano, 2019; Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il regolamento europeo 2016/679*, Torino, 2016; Rescigno, *La Carta dei diritti fondamentali dell'Unione europea*, Torino, 2003; Resta, *Autonomia privata e diritti della personalità*, Napoli, 2005; Resta, *Diritti fondamentali e diritto privato nel contesto digitale*, in *I diritti fondamentali in Europa e il diritto privato*, (a cura di) Caggia-Resta, Roma, 2019, 117-134; Resta-Zeno Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, RTDPC, 2, 2018, 411-440; Ricci, *Sulla «funzione sociale» del diritto alla protezione dei dati personali,* C IMPR, 2, 2017, 586-612; Riccio-Scorza-Belisario (a cura di), *GDPR e normativa* privacy. *Commentario*, Milano, 2018; Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostru-*

Innanzitutto, la necessità di adeguare il quadro normativo al progresso tecnologico.

Infatti, la cosiddetta "Direttiva madre" in materia di trattamento dei dati personali, la dir. 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, aveva recepito un dibattito culturale e un pensiero dottrinale sviluppatosi nei decenni precedenti e delineato un modello statico di trattamento dei dati personali, ormai superato. Diversa all'epoca anche la tecnologia: era un mondo privo di *smartphone*, *social network* e motori di ricerca. Il modello normativo individuava un unico scambio di dati: dall'interessato al titolare del trattamento. La realtà dei *social network* e dei motori di ricerca, in un mondo digitalmente sempre interconnesso, invece, si basa su un modello di condivisione e di cogestione di dati e informazioni, destinati fin dall'origine ad una circolazione globale.

Anche se il Regolamento appare già oggi in parte inadeguato a disciplinare alcuni fenomeni, come per esempio l'intelligenza artificiale, esso costituisce un avanzamento rispetto alla Direttiva.

In secondo luogo, ha determinato l'emanazione del Regolamento l'esigenza di uniformazione del quadro normativo europeo.

Come illustrato nel considerando 9 dello stesso Regolamento, esso nasce anche dalla constatazione della frammentazione della disciplina sulla protezione dei dati personali nell'Unione europea e dalla rilevazione della diffusa incertezza giuridica concernente l'applicazione della normativa.

Si è passati dalla direttiva, uno strumento di armonizzazione, che richiede l'emanazione di una normativa di attuazione da parte degli Stati membri, al re-

---

zione del fenomeno, D INF, 4, 2018, 689-726; Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno,* in *I dati personali nel diritto europeo*, (a cura di) Cuffaro-D'Orazio-Ricciuto, Torino, 2019, 23-34 e 45-60; Ricciuto, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato,* in *Persona e mercato dei dati. Riflessioni sul GDPR*, (a cura di) Zorzi, Milano, 2019, 95-136; Rodotà, *Tecnologie e diritti*, Bologna, 1995; Rodotà, *Il terribile diritto. Studi sulla proprietà privata e i beni comuni*, Bologna, 2013; Scorza, *Sub. Art. 1,* in *GDPR e normativa* privacy. *Commentario*, (a cura di) Riccio-Scorza-Belisario, Milano, 2018, 5-9; Scalisi, *L'ermeneutica della dignità*, Milano, 2018; Sica-D'Antonio-Riccio (a cura di), *La nuova disciplina europea della privacy*, Milano, 2016; Stanzione, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, EUR DIR PRIV, 2016, 1249-1264; Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice privacy*, Milano, 2019; Vettori, *I principi comuni del diritto europeo dalla Cedu al Trattato di Lisbona*, RDC, 1, 2010, 115-132; Warren-Brandeis, *The right to privacy*, 4 HARVARD LAW REV, 1890, 193-220; Zatti, *La dignità dell'uomo e l'esperienza dell'indegno*, NGCC, 6, 2012, 377-380; Zorzi (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019.

golamento, che dovrebbe essere uno strumento di uniformazione del diritto per gli Stati europei, per eliminare in radice quelle piccole differenze che rendono difficile realizzare compiutamente un mercato unico.

L'obiettivo perseguito è dunque quello di assicurare un'applicazione omogenea della normativa vigente, al fine di creare un clima di fiducia per lo sviluppo economico negli ambienti *on line*. Un quadro giuridico incerto costituisce, infatti, un freno allo sviluppo dell'economia digitale.

Come con molti altri atti normativi europei in questo settore, con esso si intende rafforzare la fiducia nelle transazioni elettroniche nel mercato interno, assicurando la protezione dei dati personali, e aumentando così l'efficacia dei servizi *on line* pubblici e privati nell'Unione europea.

Peraltro, in questo quadro, non si può non considerare il Regolamento (UE) 2014/910 del Parlamento europeo e del Consiglio del 23 luglio 2014, "in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE". I due regolamenti, considerati in una prospettiva unitaria, indicano chiaramente l'intento del legislatore europeo di disegnare un mercato unico digitale, rimuovendo gli ostacoli giuridici costituiti dalla disomogeneità delle norme applicabili.

Infine, emerge, la volontà del legislatore europeo di consolidare la posizione europea nel quadro globale, affermando un approccio unitario, che declina i principi fondamentali statuiti dalla Carta dei diritti fondamentali dell'Unione europea.

2. L'oggetto del Regolamento

L'oggetto del Regolamento in commento è spesso riassunto con il termine "privacy". Questo termine, comunque lo si pronunci, è oramai polisenso e indica una molteplicità di beni giuridici e di interessi suscettibili di differente tutela.

Innanzitutto il bene della riservatezza in senso stretto, cioè la tutela della vita privata. La segretezza, in alcuni casi. La privatezza dello spazio, in altri. La protezione delle informazioni, in altri ancora. La pluralità e la diversità dei beni giuridici considerati si riflettono anche nella scelta del legislatore europeo di disciplinare in maniera distinta la tutela della vita privata e la protezione dei dati personali, rispettivamente nell'art. 7 e nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea[2].

Ivi si afferma il diritto alla protezione dei dati personali, e precisamente che ogni individuo ha diritto alla protezione dei dati di carattere personale che lo ri-

[2] Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2102.

guardano. Si dispone, inoltre, che i dati personali devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o ad un altro fondamento legittimo previsto dalla legge e che ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Sempre nell'art. 8 si conclude che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Tale diritto è distinto dal diritto alla protezione della vita privata, altra formulazione del diritto alla riservatezza, riconosciuto dall'art. 7 della Carta, ove si afferma il diritto al rispetto della vita privata e della vita familiare: ogni individuo, dispone la norma, ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

Il diritto alla protezione dei dati personali ha un oggetto estremamente vasto, che è conseguenza della stessa definizione di dato personale.

Infatti, l'ambito individuato dalla definizione di dato personale, dettata dall'art. 4, § 1 del Regolamento, è amplissimo: costituisce dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato'); si considera 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 *on line* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». Sono, invece, esclusi dall'ambito di applicazione della normativa i dati anonimi, definiti dal considerando § 26 del Regolamento come «informazioni che non si riferiscono a una persona fisica identificata o identificabile» o «dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato».

Muovendo, dunque, dall'ampia definizione di dato personale, il diritto alla protezione dei dati personali si configura come il diritto di un soggetto di controllare l'insieme delle informazioni che a questi si riferiscono e che quindi costituiscono il suo riflesso e delineano lo stesso suo essere nella società dell'informazione, come aveva affermato Rodotà, allora Presidente dell'Autorità Garante per la protezione dei dati personali, sulla nozione di "corpo elettronico", nella Relazione 2002 sull'attività dell'Autorità Garante per la protezione dei dati personali.

Il diritto alla protezione dei dati personali è anche noto come "*information privacy*", "*informational privacy*", "*data privacy*", tutte espressioni nelle quali si evidenzia che l'oggetto del diritto è l'informazione o il dato, benché a rigore dato e informazione siano termini non coincidenti.

Il diritto alla protezione dei dati personali deve essere considerato distinto dalla libertà negativa di non subire interferenze nella propria vita privata, al cuore del diritto alla riservatezza, costituendo invece il fondamento della libertà positiva di esercitare un controllo sul flusso delle proprie informazioni. Per que-

sta ragione è frequente che il diritto alla protezione dei dati personali sia inteso come diritto all'autodeterminazione informativa, cioè alla scelta di ogni soggetto di autodefinirsi e determinarsi.

Com'è noto, il diritto alla riservatezza è, invece, il diritto di creazione giurisprudenziale consistente nell'escludere altri dalla conoscenza di vicende strettamente personali e familiari. A differenza del diritto alla protezione dei dati personali è un diritto a contenuto negativo, quello di non fare conoscere e di mantenere riservate alcune informazioni, piuttosto che a contenuto positivo, quello cioè di esercitare un controllo sulle medesime. Inoltre, a differenza del diritto alla protezione dei dati personali, non ha ad oggetto le informazioni, di qualunque natura esse siano, ma soltanto le vicende riservate.

Il diritto alla riservatezza viene generalmente ricondotto al famoso articolo di Warren e Brandeis sul '*right to be let alone*'[3] inteso come riconoscimento della inviolabilità della sfera personale e della propria vita privata. Ma da autorevole parte della dottrina viene ricondotto alla dottrina tedesca[4].

In Italia, il diritto alla riservatezza è stato riconosciuto dalla Corte di Cassazione nel 1975 (CC 27 maggio 1975 n. 2129, MGI 1975, 594), mentre la stessa Corte con la sentenza n. 4487 del 1956 aveva negato tale diritto (CC, I, 22 dicembre 1956 n. 4487, GI 1957, I, 366).

Con la pronuncia del 1975, la Corte individua il fondamento del diritto alla riservatezza nelle norme ordinarie e costituzionali che tutelano aspetti peculiari della persona, nonché nelle disposizioni, rinvenibili in leggi speciali, che richiamano espressamente la vita privata della persona. Si legge nella motivazione della sentenza: «il nostro ordinamento riconosce il diritto alla riservatezza che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificati da interessi pubblici preminenti». Successivamente, con la sentenza del 9 giugno 1998 n. 5658, la Corte di Cassazione ha sottolineato che le vicende oggetto della riservatezza si riferiscono ad una «certa sfera della vita individuale e familiare, all'illesa intimità

---

[3] Warren-Brandeis, *The right to privacy*, 4 Harvard Law Review, 1890, pp. 193-220.

[4] Per tutti, Busnelli, *Nota introduttiva al commento della l. 31 dicembre 1996 n. 675. Spunti per un inquadramento sistematico*, in *Tutela della privacy. Commentario alla l. 675/96* (a cura di) Bianca-Busnelli-Bellelli-Luiso-Navaretta-Patti-Vecchi, Padova, 1999, pp. 228-233; per un inquadramento sistematico del diritto alla riservatezza, Auletta, *Riservatezza e tutela della personalità*, Milano, 1978 e Resta, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 209.

personale in certe manifestazioni della vita di relazione, a tutte quelle vicende cioè, il cui carattere intimo è dato dal fatto che esse si svolgono in un domicilio ideale, non materialmente legato alle mura domestiche».

Come già anticipato, il diritto alla riservatezza è riconosciuto a livello internazionale dalla Convenzione di Strasburgo e dall'art. 7 della Carta dei diritti fondamentali dell'Unione europea. A livello universale, l'art. 12 della Dichiarazione universale dei diritti dell'uomo, ripreso in termini quasi identici dall'art. 17 del Patto sui diritti civili e politici del 1966, sancisce che «nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesioni del suo onore e della sua reputazione».

Il diritto alla protezione dei dati personali e il diritto alla riservatezza hanno ambiti molto diversi e soprattutto hanno oggetti diversi. Naturalmente ci sono dei casi in cui i due diritti coincidono.

Nell'ordinamento giuridico italiano, come è noto, il diritto alla protezione dei dati personali è stato introdotto con la l. 31 dicembre 1996, n. 675, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" ed è stato sancito dall'art. 1, oggi abrogato, del d.lgs. 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", che recita: «chiunque ha diritto alla protezione dei dati personali che lo riguardano»[5].

Dunque da almeno venti anni il diritto alla protezione dei dati personali è positivamente riconosciuto e distinto dal diritto alla riservatezza.

Benché dunque il Regolamento sia noto come "regolamento sulla *privacy*" esso non ha ad oggetto il diritto alla riservatezza: ha un ambito molto più ampio della riservatezza, ma che non è necessariamente connesso alla sfera più intima della persona. I dati personali costituiscono il tema disciplinato anche se non si riferiscono a vicende private, intime o familiari. Qualunque informazione, quale che sia il suo contenuto, è oggetto del Regolamento.

Il Regolamento dunque ha un contenuto molto ampio e disciplina temi che nulla hanno a che fare con la riservatezza in senso stretto, ma che attengono invece al regime di circolazione delle informazioni, in parte propri di altri settori e materie, quali il mercato della concorrenza sulle informazioni e l'accesso alle informazioni.

Ne è un esempio l'introduzione del diritto alla portabilità dei dati, cioè il diritto dell'interessato «di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e (…) di trasmettere tali dati a un altro titolare del trat-

[5] Per un inquadramento dell'evoluzione del diritto alla *privacy* che ha portato alla elaborazione di un distinto diritto alla protezione dei dati personali, Busnelli, cit.

tamento senza impedimenti da parte del titolare del trattamento cui li ha forniti» (art. 20 del Regolamento). Esso rivela una chiara matrice *antitrust* e garantisce, in primo luogo, la concorrenza fra diversi operatori del mercato, a partire dai *social network*, con riferimento ai quali è nato.

3. Il titolo del Regolamento

Il Regolamento europeo 2016/679 attiene, come recita il titolo, «alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati». Già la direttiva 95/46 del 24 ottobre 1995 era relativa, come recitava il titolo, «alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati». Lievi sfumature a conferma del duplice oggetto invariato: insieme la protezione dei dati personali e la libera circolazione dei dati.

Il legislatore italiano, invece, fin dalle prime disposizioni in materia, ha posto l'accento soltanto su uno dei due termini dell'espressione, quello costituito dalla protezione dei dati personali. Già la prima legge italiana in materia di protezione dei dati personali, la l. 31 dicembre 1996, n. 675, abrogata, era infatti intitolata «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali» e non menzionava nel titolo la libera circolazione dei dati.

Significativa la scelta del legislatore italiano il quale nell'omettere il riferimento alla libera circolazione dei dati personali ha effettuato una scelta che ha poi segnato un netto orientamento successivo, costituito dal concentrarsi in maniera pressoché esclusiva sulla protezione dei dati personali. Analogamente, il Garante per la protezione dei dati personali italiano, il quale ha attribuito un ruolo assolutamente marginale alla libera circolazione dei dati.

Lo scenario italiano è dunque fortemente condizionato, fin dall'inizio, dalla netta indicazione legislativa. Ciò spiega alcune difficoltà oggi persistenti nell'interpretazione del Regolamento e la difficoltà attuale ancora permanente nell'applicazione del criterio del bilanciamento[6].

4. Il duplice oggetto e la necessità del bilanciamento

Il duplice oggetto è dunque enunciato nel titolo e poi ribadito nel primo comma dell'articolo di apertura del Regolamento europeo.

---

[6] Tale lettura asimmetrica delle due anime della normativa europea è rilevata da Scorza, *Sub. Art. 1, in GDPR e normativa privacy. Commentario* (a cura di) Riccio-Scorza-Belisario, Milano, 2018, p. 5.

Esso riflette una duplice esigenza di natura politica cui si è fatto cenno: da un lato, confermare il modello europeo di protezione dei diritti fondamentali, in contrapposizione al modello statunitense e a quello cinese; dall'altro, promuovere il mercato digitale europeo. In quest'ultima direzione si attesta anche il già citato Reg. UE n. 2014/910 («eIDAS») del Parlamento europeo e del Consiglio del 23 luglio 2014, «in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE» il quale promuove il mutuo riconoscimento di identità digitali, firme elettroniche e servizi fiduciari, nell'intento di favorire il consolidamento del mercato unico europeo.

Com'è noto, il bene sul quale si fonda il nuovo mercato è costituito dalle informazioni, delle quali, dunque, il legislatore europeo non può che favorire la circolazione, per sostenere il mercato europeo.

Fra esigenza di protezione dei dati personali e libera circolazione delle informazioni occorre dunque definire un equilibrio. In questo esercizio difficile e complesso si muove il legislatore europeo anche con riguardo al tema più attuale, quello dello sviluppo dell'intelligenza artificiale, nel quale pure procede con un passo costante, attento a non trascurare né l'esigenza di tutelare il diritto fondamentale alla protezione dei dati personali, né l'urgenza di costruire e rafforzare il mercato unico digitale europeo (ci si riferisce allo «spazio dei dati europeo» già nella comunicazione della Commissione europea *L'intelligenza artificiale per l'Europa* COM 2018 237, 25 aprile 2018, p. 11 ove l'esigenza di disporre di dati personali viene controbilanciata dalla necessità di assicurare il pieno rispetto della legislazione sulla protezione degli stessi. Nello stesso senso anche COM 2018 795 e l'allegato alla stessa, intitolato *Piano coordinato per lo sviluppo e l'utilizzo dell'intelligenza artificiale "*Made in Europe*"*, p. 14, nonché la Risoluzione del Parlamento europeo del 12 febbraio 2019. Più di recente, la Risoluzione approvata il 21 gennaio 2020 dalla *Committee on the Internal Market and Consumer Protection* del Parlamento europeo, e il Comitato economico e sociale europeo col parere *Creare fiducia nell'intelligenza artificiale antropocentrica* pubblicato nella G.U.U.E. dell'11 febbraio 2020).

A ben vedere, non è solo quello segnalato nel titolo del Regolamento il confronto cui esso è destinato, anzi i termini entro i quali la necessaria dialettica si sviluppa sono molteplici[7].

Tutto il Regolamento è intrinsecamente caratterizzato dall'esigenza di bilanciamento fra diritti e interessi in confronto. Ciò è l'esito logico innanzitutto dalla stessa definizione di dato personale che è, di per sé, onnipervasiva, come sopra si è illustrato.

---

[7] Sul bilanciamento fra principi, Gambaro, *Categorie del diritto privato e linguaggio delle carte dei diritti fondamentali, in I diritti fondamentali in Europa e il diritto privato* (a cura di) Caggia-Resta, Roma, 2019, pp. 43-64.

Il dato personale è definito dal legislatore come qualunque informazione direttamente o indirettamente riferibile ad una persona fisica, cosicché l'ambito di applicazione del Regolamento finisce con l'essere quello costituito dalle informazioni, salvo l'eccezione costituita dal dato anonimo. Il Regolamento si espande dunque orizzontalmente, a pervadere ogni relazione giuridica, e non verticalmente, alla stregua di una disciplina di segno esclusivamente specialistico. E allora nel suo espandersi incontra altri diritti e altre situazioni giuridiche soggettive con le quali è necessario un confronto.

Ciò risulta evidente dal considerando § 4 del Regolamento che recita: «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 medesimo considerando precisa che il Regolamento «rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, e enumera i diritti fra i quali può generarsi un potenziale conflitto: 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»[8].

Non diversamente si era espressa la nostra Corte di Cassazione in particolare nella sentenza n. 10280/2015 della Sezione III, ove si afferma che il diritto alla protezione dei dati personali, qualificato come pretesa ad esigere una corretta gestione dei propri dati personali, pur rientrando nei diritti fondamentali della persona, non è un «*totem* al quale possano sacrificarsi altri diritti altrettanto rilevanti sul piano costituzionale» e, conseguentemente, la disciplina in materia «va coordinata e bilanciata da un lato con le norme che tutelano altri e *prevalenti* diritti (tra questi, l'interesse pubblico alla celerità, trasparenza ed efficacia all'attività amministrativa); dall'altro, con le norme civilistiche in tema di negozi giuridici» (CC, III, 20 maggio 2015 n. 10280, DR 2015, 10, 969).

Il diritto alla protezione dei dati personali si configura così come un diritto fondamentale ma non assoluto, che richiede sempre un necessario confronto e una necessaria modulazione con altri diritti.

Questo è a ben vedere il cuore del Regolamento europeo che non soltanto ha posto il bilanciamento al centro, ma che sul bilanciamento è addirittura imperniato. In questo senso aveva già mosso qualche passo, invero un po' sbilanciato verso la protezione della vita privata e la protezione dei dati personali, coniuga-

[8] Cfr. Ricci, *Sulla "funzione sociale" del diritto alla protezione dei dati personali*, in C IMP, 2, 2017, pp. 586-612.

te indissolubilmente in un'endiadi spesso solo retorica, la giurisprudenza della Corte di Giustizia europea: basti ricordare per tutte la decisione *Google Spain* (il riferimento è alla CGUE 13 maggio 2014 C-131/12)[9].

Oggi si è modificato il baricentro della normativa sulla protezione dei dati personali, che non può essere vista come fosse chiusa su sé stessa, ma invece sempre e necessariamente in relazione con altri diritti.

La dialettica fra la protezione dei dati personali e la libera circolazione delle informazioni non può che snodarsi lungo alcune direttrici fondamentali: occorre verificare di volta in volta se si tratti di situazioni giuridiche di pari portata; non pare si possa giungere ad una conclusione di carattere generale ma invece sembra che l'esito sia da determinarsi caso per caso e, infine, che l'equilibrio sia mutevole e non possa che essere individuato dinamicamente, caso per caso.

Occorre inoltre sciogliere quell'endiadi cui si è prima fatto cenno che ricorre sovente anche nelle decisioni della Corte di Giustizia europea costituita dal diritto alla protezione dei dati personali e dal diritto alla protezione della vita privata.

Si tratta spesso di una mera citazione di stile, che non suscita una particolare autonoma attenzione, ma che consente di fare prevalere il diritto alla protezione dei dati personali sugli altri diritti. Per operare correttamente un bilanciamento, l'endiadi deve essere sciolta e verificata caso per caso. In taluni casi il diritto alla protezione dei dati personali sarà associato alla protezione della vita privata, in particolare quando si tratta di tutela la riservatezza, in altri no.

Invero non sembra sempre essere la vita privata il bene che si vuole proteggere, quanto piuttosto le informazioni, e più o meno consapevolmente, il valore economico ad esse connesso. Il diritto alla protezione dei dati personali è talmente pervasivo da superare agevolmente i confini della vita privata in senso stretto e da approdare nel mercato digitale delle informazioni *on line*.

5. Due visioni sottese

I due termini della relazione stabilita dal Regolamento, protezione delle persone fisiche con riguardo al trattamento dei dati personali e libera circolazione dei dati, sottintendono due concezioni, l'una personalistica e l'altra patrimonialistica.

Il riferimento alla protezione delle persone fisiche con riguardo al trattamento dei dati personali inquadra il tema nella cornice classica dei diritti della personalità. Il riferimento alla libera circolazione dei dati invece sottende la concezione del dato come bene giuridico oggetto di scambio.

---

[9] Sul punto, si rinvia a Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali: da Google Spain a Schrems*, in D INF, 4-5, 2015, pp. 779-799.

Il dato personale ha da sempre una duplice natura: da un lato è la proiezione della personalità dell'individuo, l'oggetto del diritto fondamentale riconosciuto dall'art. 8 della Carta europea dei diritti fondamentali; dall'altro può essere considerato bene giuridico economicamente valutabile e oggetto di scambio. Fin troppo ovvio ricordare che nella società dell'informazione, i dati personali che sono informazioni riferibili a persone fisiche, sono beni. Quando i dati costituiscono oggetto di scambio, si profila quindi un contrasto fra la realtà commerciale internazionale e la concezione teorica tradizionale che afferma l'indisponibilità dei diritti della personalità[10].

Tale ambivalenza è esplicitamente dichiarata nel Regolamento (UE) 2016/679 fin dal titolo, come già commentato. Ora una difficoltà culturale, prima ancora che giuridica, risiede nell'accettare la circolazione e quindi lo scambio della proiezione di un diritto della personalità. Inutile ricordare che la categoria dei diritti della personalità si caratterizza anche per l'indisponibilità dei diritti, che non significa, come è stato ampiamente e approfonditamente chiarito, indisponibilità all'esercizio dei diritti[11].

Permane una resistenza culturale che rende difficilmente accettabile che il dato personale possa essere oggetto di scambio. Sul punto il Garante europeo della protezione dei dati personali, nell'ambito della sua *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content* del 14 marzo 2017, aveva segnalato «l'importanza di un'economia basata sui dati per la crescita nell'Unione europea», contestualmente affermando che «i diritti fondamentali, come il diritto alla protezione dei dati personali, non possono essere ridotti a semplici interessi dei consumatori e i dati personali non possono essere considerati una mera merce», mettendo in dubbio la legittimità dell'uso dei dati come controprestazione[12]. Il tema è stato poi recentemente affrontato anche dall'Autorità garante della concorrenza e del mercato (per brevità, "AGCM") che, tra le altre pratiche scorrette imputate al noto *social network* Facebook, ha rilevato in particolare l'utilizzo per fini commerciali dei dati degli utenti, i quali, in modo inconsapevole e automatico,

---

[10] Cfr. Resta, cit.

[11] Cfr. Resta-Zeno Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *RTDPC*, 2, 2018, pp. 411-440; Resta, *Diritti fondamentali e diritto privato nel contesto digitale,* in (a cura di) Caggia-Resta, op. cit., pp. 117-134.

[12] Sulla patrimonializzazione dei dati personali, si rinvia a Ricciuto, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, in *Persona e mercato dei dati. Riflessioni sul GDPR* (a cura di) Zorzi, Milano, 2019, pp. 95-136.

consentivano il trasferimento dei propri dati a terzi operatori tramite un sistema di preselezione del consenso alla cessione e all'utilizzo dei dati, ed erano altresì indotti a mantenere attivo tale trasferimento al fine di evitare di subire limitazioni nell'utilizzo del servizio, conseguenti alla deselezione (AGCM 29 novembre 2018 n. 27432; 21 gennaio 2020 n. 28072). A conferma dell'ingannevolezza della pratica commerciale in esame è intervenuto anche il T.A.R. Lazio secondo cui «[…][i]l fenomeno della 'patrimonializzazione' del dato personale, tipico delle nuove economie dei mercati digitali, impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione ad un contratto per la fruizione dei un servizio, quale è quello di utilizzo di un '*social network*'». Alla luce di tali riflessioni, il giudice amministrativo ha ritenuto «corretta la valutazione della Autorità [garante della concorrenza e del mercato] circa l'idoneità della pratica a trarre in inganno il consumatore e a impedire la formazione di una scelta consapevole, omettendo di informarlo del valore economico di cui la società beneficia in conseguenza della sua registrazione al *social network*» (TAR Lazio, I, 18 dicembre 2019 n. 260 e n. 261).

La problematica che qui si è prospettata ne porta con sé anche un'altra relativa alla natura, negoziale o autorizzatoria, del consenso come base giuridica legittimante il trattamento. Questa problematica è amplissima e non può essere trattata in questa sede[13].

Non consente di afferrare la complessità del tema riferire solo alla categoria dei diritti della personalità tutto il fenomeno sociale ed economico che ruota intorno alle informazioni di carattere personale, ma occorre invece prendere atto della complessità e cercare di procedere verso una razionalizzazione fra diritti della personalità e disciplina del contratto.

Analogamente appare del tutto inadeguato il paradigma proprietario per definire i diritti del soggetto al quale i dati si riferiscono oppure, al contrario, il soggetto che li ha raccolti.

A differenza di quanto avverte il comune sentire, non esiste un vero e proprio "proprietario" del dato personale, ma il dato è al centro di una fitta rete di relazioni fra una pluralità di soggetti diversi, che detengono specifici diritti o

[13] Il tema è inoltre affrontato da Alpa, *La 'proprietà' dei dati personali*, in (a cura di) Zorzi, op. cit., pp. 11-34 e da Bravo, *Le condizioni di liceità del trattamento di dati personali*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018 n. 101*, (diretto da) Finocchiaro, Bologna, 2019, pp. 110-193.

doveri in relazione al dato stesso. La prima figura a cui si pensa è ovviamente quella dell'interessato del trattamento che, semplificando, possiede quel generale diritto di "controllo" sul dato, che poi altro non è se non il contenuto concreto del diritto alla protezione dei dati personali. Tale potere di controllo si estrinseca nei diversi diritti previsti dal Regolamento quali il diritto di opposizione al trattamento, il diritto all'oblio, il diritto di accesso, il diritto di rettifica, il diritto di cancellazione dei dati, e così via. Altra figura fondamentale è ovviamente quella del titolare del trattamento. Ma il titolare nel Regolamento è innanzitutto il soggetto su cui gravano obblighi e responsabilità.

Con diverso significato, di "titolare" si parla anche nel d.lgs. 7 marzo 2005, n. 82 Codice dell'amministrazione digitale" (di seguito anche "CAD") e nella l. 22 aprile 1941, n. 633 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio", testi normativi nei quali possiamo trovare altre interessanti prospettive. Il CAD, infatti, individua il titolare quale il «soggetto che ha formato per uso proprio il documento che rappresenta il dato o che ne ha la disponibilità». La l. 633/1941 invece fa riferimento al titolare di un diritto sulle c.d. "banche di dati". Si tratta quindi o del diritto "*sui generis*" per il contenuto di banche di dati con rilevanti investimenti in termini finanziari, di tempo o di lavoro umano oppure dei diritti di proprietà intellettuale per la struttura di banche dati frutto del lavoro intellettuale del titolare.

Dunque, non un diritto di proprietà, ma diversi diritti, non esclusivi. L'approccio proprietario, proprio sotto quest'ultimo profilo, si rivela del tutto inadeguato.

I dati personali sono invece oggetto di fruizione da parte di una pluralità di soggetti e come accade per i beni immateriali, possono essere utilizzati più e più volte. Il possesso è il potere di disporne, non la disponibilità materiale.

La medesima informazione viene utilizzata da più soggetti per scopi e finalità diverse, su basi giuridiche differenti.

Il ragionamento giuridico, dunque, non deve essere impostato come diritto di disporre in modo pieno ed esclusivo, ma piuttosto come un diritto di utilizzo che attinga agli strumenti della proprietà intellettuale[14].

---

[14] Con più ampio respiro, riguardo alla crisi della teoria generale del bene, Lipari, *Le categorie del diritto civile*, Milano, 2013, spec. pp. 122-127, in cui l'A. scrive che il «concetto di bene giuridico sempre più di frequente non preesiste alla qualificazione giuridica limitandosi il diritto a comporre gli interessi (della più varia natura) che si indirizzano al medesimo bene ma viene creato in funzione degli interessi». Ed ancora: «il bene emerge in chiave giuridica in conseguenza della proiezione dinamica del soggetto a realizzare un certo interesse. E l'interesse a sua volta deve essere inteso come tensione del soggetto a creare il bene a far nascere una rilevanza giuridica altrimenti inesistente».

6. Il limite del Regolamento nella tutela della persona

Il Regolamento soffre di un limite che è connaturato all'impostazione stessa del problema che intende risolvere: non si guarda alla persona, ma al dato che alla persona si riferisce.

Il diritto alla protezione dei dati personali e il Regolamento che lo disciplina tutelano l'informazione riferita o riferibile all'individuo. Non tutelano la personalità nel suo complesso. Proteggono il frammento, non l'insieme.

La tutela dell'individuo nel suo complesso è invece affidata in Italia principalmente al diritto all'identità personale, come è noto di creazione giurisprudenziale, che appare quasi marginale a confronto con un corpo normativo di 173 considerando e 99 articoli. Questo diritto, sconosciuto ad altri ordinamenti, che ha dato luogo a decisioni innovative della nostra giurisprudenza che ha affermato il diritto all'oblio e alla contestualizzazione delle informazioni (CC 5 aprile 2012 n. 5525, FI. 2013, I, 305;[15] andrebbe invece valorizzato per consentire di considerare l'identità nel suo complesso e non soltanto un suo frammento. È il percorso che ha intrapreso la giurisprudenza della Suprema Corte nella menzionata decisione 5525/2012 sul diritto all'oblio, in cui ha evidenziato il profilo del diritto alla contestualizzazione dei dati personali.

7. Un sistema in costruzione

Il diritto alla protezione dei dati personali oggi delinea un sistema normativo multilivello che appare ancora ben lungi dall'essere completo. Ci troviamo, quindi, davanti alla costruzione di un edificio normativo che si vorrebbe sistematico ma che è ancora lontano dall'avere raggiunto compiutamente questo obiettivo.

Il Regolamento europeo sulla protezione dei dati personali del 2016 ha riscritto la normativa nazionale, quindi ha rivisto, in alcuni casi completamente, delle norme che si erano già consolidate in ambito italiano. Nel riscrivere, però, queste disposizioni, il testo normativo europeo non si è collocato, evidentemente, in un'area completamente sgombra di esperienze, di discipline di vario ordine e di culture e di valori. Il Regolamento europeo, dunque, ha riscritto ma in un contesto che era già altamente definito e maturo.

---

[15] Si affronta ampiamente tale tema in Finocchiaro, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, in D INF, 3, 2012, pp. 383-394. Sul diritto all'oblio invece *cfr.* Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, in D INF, 4-5, 2014, pp. 591-604.

Siamo davanti ad un sistema in costruzione e ad alta complessità: già sulla parola *privacy* e sui suoi molteplici significati si può non concordare. Come si è illustrato, con la parola *privacy* si possono intendere tante cose diverse: dalla riservatezza, alla protezione dei dati personali. All'interno delle esigenze di tutela che la normativa esprime non ci sono soltanto quelle di protezione della persona fisica, ma spesso ci sono necessità completamente diverse: basti pensare alle esigenze espresse dal diritto alla portabilità dei dati, da leggere in un'ottica *antitrust* e di tutela della concorrenza.

Questo sistema è ben lungi dall'essere stato già edificato: è un edificio che presenta molte aperture e molti cantieri aperti, alcuni dei quali segnalati dallo stesso Regolamento. Peraltro il Regolamento, per certi aspetti, come è stato notato da molti commentatori, presenta le caratteristiche di una direttiva: rinvia agli interventi degli Stati nazionali. Nato per assicurare certezza e per costruire il mercato unico digitale europeo, è riuscito in questo intento solo in parte, perché ci sono molti capitoli che lasciano, invece, spazio al legislatore nazionale.

Oltre a questo, il sistema che si sta costruendo si inserisce in un contesto già molto maturo e molto consolidato. Non si può non richiamare il principio di tutela della dignità, che certamente era nel Codice *privacy* ma, ben prima, era ed è nella Carta dei diritti fondamentali: nel contesto europeo di tutela dei diritti fondamentali va letto il Regolamento europeo[16].

Il quadro normativo risultante è un quadro composito, costituito da molteplici livelli normativi e paranormativi, di *hard* e di *soft law*. Non è ancora un sistema, ma richiede il lavoro e l'impegno della dottrina e della giurisprudenza per diventarlo.

Si muove dalle fonti europee, dalla Carta dei diritti fondamentali e in particolare dagli artt. 1, 7 e 8: la tutela della dignità, della protezione della vita privata e della protezione dei dati personali. Questi principi sono declinati nel Regolamento europeo. Si aggiungono le disposizioni del Codice per la protezione dei dati personali, modificato, e del d. lgs. 101/2018. Il quadro va quindi integrato con i provvedimenti del Garante e con le disposizioni dei codici deontologici e di settore. La lettura del quadro verrà completata dalle opinioni dell'*European Data Protection Board* e dalle pronunce del Garante. Fin qui i contorni del sistema considerato come normativa speciale. Ma ciò che spesso si trascura, commettendo l'errore del neofita che si concentra solo sulla novità, è che il sistema della protezione dei dati personali deve essere inquadrato nel più ampio sistema della tutela della persona,

[16] Sulla dignità, Busnelli, *Le alternative sorti del principio di dignità della persona umana*, in RDC, 5, 2019, pp.1071-1085; Scalisi, *L'ermeneutica della dignità*, Milano, 2018; Zatti, *La dignità dell'uomo e l'esperienza dell'indegno*, in NGCC, 6, 2012, pp. 377-380.

muovendo dalla dignità, sancita dalla Carta europea, fino alla tutela dell'identità personale nella sua più recente declinazione di diritto alla contestualizzazione dei dati, affermata dalla giurisprudenza italiana (CC 5 aprile 2012 n. 5525, FI 2013, I, 305). Questo sistema normativo va calato in un sistema più ampio e più complesso, con il quale deve confrontarsi, per trovare un'applicazione che passi inevitabilmente per un bilanciamento. Il diritto alla protezione dei dati personali è un diritto che si sviluppa nella comunicazione e che si declina nella relazione. Non è un diritto statico, ma si compie nella dinamicità del confronto. Trova dunque anche le sue limitazioni e il suo contenuto nella dialettica con altri diritti.

Ora, in questo esercizio di costruzione e di edificazione del sistema, certamente le Corti hanno un ruolo fondamentale. Si è instaurato un dialogo non necessariamente consapevole e comunque un alternarsi di decisioni anche di segno diverso. Si segnala, per esempio, nel contesto italiano, quello fra la Corte di Cassazione e la Corte di Giustizia europea. Alcuni spazi, quindi, si stanno riempiendo per l'azione delle Corti, sia della Corte di Giustizia europea, sia della nostra Corte di Cassazione.

Si alternano visioni diverse nell'ambito della stessa Corte di Giustizia europea, che non è omogenea nel suo procedere e che nel definire alcuni diritti ha alternato diverse visioni nella sentenza del 2014 (CGUE 13 maggio 2014 C-131/12) e nelle sentenze gemelle del 2019 (CGUE 24 settembre 2019 C-507/17 e C-136/17). Analogamente, anche la nostra Corte di Cassazione ha avvertito l'esigenza di una pronuncia a sezioni unite con riguardo al tema attuale del diritto all'oblio (CC, SU, 22 luglio 2019 n. 19681, FI 2019, 10, 1, 3071).

Dunque un dialogo serrato fra Corti e all'interno delle stesse Corti, per costruire quel sistema che oggi è composto da molti livelli di norme non ancora armonizzati in una prospettiva soddisfacente per l'interprete.

Un sistema che da un lato non si limiti a considerare un solo diritto, il diritto alla protezione dei dati personali, ma invece i diritti della persona (fra i quali soprattutto il diritto alla riservatezza e il diritto all'identità personale) per tutelare la persona nella sua interezza e dall'altro lato consideri il mercato, nel quale le informazioni e anche i dati personali circolano.

Un sistema che individui un paradigma diverso da quello proprietario, dal momento che l'esclusività del diritto di godere e di disporre in questo caso non può trovare spazio, e che piuttosto attinga agli strumenti della proprietà intellettuale e definisca non una proprietà ma un diritto di utilizzo dei nuovi beni. In taluni casi, beni comuni[17].

[17] Sul punto si rinvia per tutti a Rodotà, *Il terribile diritto. Studi sulla proprietà privata e i beni comuni*, Bologna, 2013.

8. L'adeguamento della normativa italiana al Regolamento europeo

L'entrata in vigore del Regolamento ha reso inevitabile la verifica di compatibilità delle norme italiane rispetto a quelle europee che ovviamente le sostituiscono.

La verifica può essere effettuata dagli interpreti, dagli operatori del diritto e naturalmente e *in primis* dai giudici e dal Garante per la protezione dei dati personali.

Il legislatore italiano, tardivamente, ha ritenuto che la verifica o quanto meno, una verifica, dovesse essere effettuata dal legislatore delegato. La legge di delegazione europea del 25 ottobre 2017, n. 163, art. 13, ha disposto in questo senso.

Il Ministero della Giustizia ha nominato solo nel dicembre 2017 una Commissione incaricata di adeguare la normativa italiana a quella europea (della Commissione, presieduta da chi scrive, hanno fatto parte molti autorevoli esperti come Oreste Pollicino, Giorgio Resta, Giovanni Guerra, Vittorio Manes e Franco Pizzetti). I lavori della Commissione sono iniziati il 4 gennaio 2018, mentre altri Paesi europei avevano iniziato analogo percorso nel 2016. I lavori hanno dovuto concludersi il 19 marzo, per consentire al Governo uscente di approvare lo schema di decreto il 21 marzo, nell'ultimo Consiglio dei ministri utile. Poi lo schema di decreto ha continuato il suo complesso percorso che si è snodato fra due Governi e due Parlamenti.

L'intento della Commissione era quello di vedere pubblicato il decreto in Gazzetta Ufficiale entro la data fatidica del 25 maggio 2018, ma purtroppo i tempi si sono dilatati.

Ciò premesso, si illustrano il metodo e le scelte principali adottati nel decreto, muovendo dai vincoli.

Come si è accennato, il decreto ha l'obiettivo di coordinare la normativa italiana con quella europea, dopo avere effettuato una verifica di compatibilità.

L'accorpamento di tutte le disposizioni in un testo unico, certamente auspicabile perché avrebbe costituito un'opera di razionalizzazione della materia e avrebbe consentito la più agevole fruibilità da parte degli operatori, non è stato ritenuto praticabile perché il Regolamento europeo deve restare come corpo normativo a sé stante, come è stato ribadito sotto l'attenta supervisione della Commissione europea (il riferimento è alla Comunicazione della Commissione europea al Parlamento europeo e al Consiglio n. COM 2018 43 *final* del 24 gennaio 2018 "Maggiore protezione, nuove opportunità – Orientamenti della Commissione per l'applicazione diretta del regolamento generale sulla protezione dei dati a partire dal 25 maggio 2018", par. 3.1).

La Commissione incaricata dal Ministero della Giustizia ha dunque proceduto a verificare se le norme del Codice *privacy* vigente fossero compatibili con quelle del Regolamento.

La legge di delega prevedeva l'abrogazione delle disposizioni del Codice *privacy* incompatibili con il Regolamento europeo, la modifica del Codice, nonché il coordinamento del quadro normativo, in osservanza del principio generale di semplificazione e riassetto normativi.

Dunque, muovendo dal Regolamento europeo, fonte sovraordinata, si è proceduto ad eliminare le disposizioni del Codice italiano, figlio della Direttiva abrogata, non compatibili col Regolamento. In conclusione, pressoché l'intera parte generale del Codice è risultata abrogata.

Lo schema di decreto di coordinamento ha dunque dichiarato la sostituzione e l'abrogazione espressa delle norme del Codice superate dal Regolamento. Così, per esempio, con riguardo alle disposizioni concernenti l'informativa, il consenso e tutta la materia della sicurezza.

Questa operazione di semplificazione ha rappresentato innanzitutto una scelta culturale. È raro che si dichiari l'abrogazione espressa delle norme e anzi tendenzialmente si procede verso l'accumulazione.

Rendere il quadro chiaro agli operatori costituisce di per sé un valore.

Se, ad esempio, fossero rimaste vigenti le disposizioni del Codice *privacy* sui temi indicati, insieme a quelle del Regolamento, gli operatori si sarebbero chiesti in quale modo combinare e integrare le diverse disposizioni, approdando come inevitabilmente accade nell'ambito giuridico a conclusioni differenti, ma generando quell'incertezza giuridica che porta con sé inutili costi e rallentamenti per gli operatori economici.

Dunque, una scelta di metodo, non frequente, volta a semplificare e a razionalizzare.

Di conseguenza, si è posta la scelta se mantenere un terzo testo normativo (oltre al Regolamento e al decreto) costituito da ciò che restava del Codice, all'evidenza non più tale, o se trasferire le disposizioni del Codice nel decreto, lasciando agli operatori non tre, ma due testi normativi. Questa seconda scelta era parsa alla Commissione la più razionale nell'ottica di riordinamento e di semplificazione.

Un dibattito tanto acceso nei toni quanto privo di consistenti contenuti giuridici ha voluto ingenerare l'equivoco che abrogare il Codice implicasse un'abrogazione o quanto meno un indebolimento del diritto disciplinato. Non si è ancora pienamente compreso che il Regolamento europeo ha riscritto la normativa sulla protezione dei dati personali: ha abrogato la Direttiva madre e sostanzialmente anche il Codice per la protezione dei dati personali italiano.

Il legislatore italiano alla fine ha scelto di mantenere la veste esteriore del Codice per la protezione dei dati personali, che molto poco ha ormai dell'organicità che un codice dovrebbe avere. Molte disposizioni sono state abrogate perché sostituite da quelle del Regolamento europeo e molte altre sono state modificate

per adeguarle a quelle del Regolamento. La tecnica normativa scelta alla fine dal legislatore non aiuta certamente la leggibilità che, di per sé, avrebbe dovuto rappresentare un valore.

Alcune norme italiane sono state modificate, per adeguarle alla nuova disciplina europea. Ad esempio, non essendo più richiesto il consenso per il trattamento dei dati sanitari per finalità di cura, sono state modificate le disposizioni in materia di sanità che lo prevedevano.

La proposta della Commissione, accolta dal legislatore, mirava, inoltre, a mantenere la continuità facendo salvi per un periodo transitorio i provvedimenti del Garante (si pensi, per esempio a quello in materia di biometria) e le autorizzazioni, oggetto di successivo riesame.

Sono stati mantenuti anche i Codici deontologici vigenti come, ad esempio, quello dei giornalisti.

Si è rafforzato il meccanismo delle consultazioni pubbliche e il coinvolgimento delle categorie interessate in molteplici casi.

Per le micro, piccole e medie imprese si è previsto che il Garante promuovesse modalità semplificate di adempimento degli obblighi del titolare del trattamento.

In attesa dell'emanando Regolamento europeo in materia di *e-Privacy*, il decreto non ha modificato le disposizioni concernenti le comunicazioni elettroniche.

Considerato il nuovo approccio europeo alla protezione dei dati personali, lo schema di decreto cercava di semplificare e deburocratizzare, nonché di ridurre i costi dell'incertezza giuridica. Il legislatore ha accolto solo in parte questa spinta.

Il legislatore italiano ha scelto alla fine di inasprire il quadro sanzionatorio penale, nonostante le severe sanzioni amministrative previste dal Regolamento europeo (fino a 20 milioni di euro o al 4% del fatturato mondiale annuale lordo), di natura sostanzialmente penale. La proposta della Commissione era, al contrario, nel senso di depenalizzare, in ossequio al principio del *ne bis in idem* sostanziale e processuale.

Federica Resta[1]

La Direttiva sulla protezione dei dati personali in ambito giudiziario penale e di polizia e la tutela dei terzi

Sommario: 1. La direttiva 2016/680. – 2. Il recepimento della direttiva. – 3. I dati personali contenuti in atti giudiziari, le intercettazioni e la tutela dei terzi.

1. La direttiva 2016/680

Una delle componenti più significative (ma, paradossalmente, anche meno conosciute) del nuovo quadro giuridico europeo in materia di protezione dei dati personali è rappresentato dalla direttiva 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, "*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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*".

La direttiva reca la disciplina – speculare a quella del Regolamento generale sulla protezione dei dati personali, (UE) 2016/679, "GDPR" – della protezione dei dati personali nell'esercizio dell'attività giudiziaria penale e di polizia, affidandola tuttavia a uno strumento giuridico di armonizzazione (e non di diretta unificazione) delle legislazioni, in ragione delle peculiarità della materia e della diversità dei sistemi processuali tra Stati membri, secondo quella specificità richiesta dalla dichiarazione 21, allegata all'atto finale della Conferenza intergovernativa che ha approvato il Trattato di Lisbona[2].

Innovando rispetto alla decisione quadro, che abroga, la direttiva estende la sua sfera applicativa dal solo ambito della cooperazione di polizia e giudiziaria a quello delle attività (giudiziaria penale e di polizia) svolte in ambito interno.

---

[1] Le opinioni contenute in questo contributo sono espresse dall'autrice a titolo esclusivamente personale e non impegnano in alcun modo l'Autorità di appartenenza.

[2] Secondo cui "*La conferenza riconosce che potrebbero rivelarsi necessarie, in considerazione della specificità dei settori in questione, norme specifiche sulla protezione dei dati personali e sulla libera circolazione di tali dati nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, in base all'articolo 16 del trattato sul funzionamento dell'Unione europea*".

La distinzione dell'ambito applicativo tra regolamento e direttiva 680 è, dunque, tutta giocata sul duplice elemento soggettivo (svolgimento del trattamento da parte di autorità nazionali competenti nelle materie individuate) e teleologico-funzionale (perseguimento di fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di, minacce alla sicurezza pubblica).

La concorrente applicazione dei due strumenti normativi, GDPR e direttiva (fondata tanto sull'elemento soggettivo quanto su quello teleologico-funzionale della preordinazione del trattamento a fini preventivi o repressivi) determina, quindi, il singolare effetto di scindere la stessa disciplina dei trattamenti svolti per fini di giustizia in due sotto-sistemi distinti. L'attività giudiziaria (corrispondente all'esercizio di funzioni requirenti e giudicanti, anche in ambito esecutivo o di sorveglianza), in sede penale è soggetta (al pari dell'attività di polizia in senso stretto), per quanto concerne la disciplina di protezione dati, alla direttiva 2016/680.

Così anche – come chiarito dal d.lgs. 18 maggio 2018, n. 51 – l'attività giurisdizionale connessa all'applicazione di misure di sicurezza e prevenzione, correlata comunque alla prevenzione di reati, è disciplinata, ai fini *privacy*, dalla direttiva (e, naturalmente, dalle norme nazionali di recepimento: per l'Italia il d.lgs. 51).

Di contro, l'attività giudiziaria svolta da ogni altra giurisdizione (anche dalla stessa autorità giudiziaria ordinaria, ma in sede civile) è attratta nell'ambito applicativo del GDPR, con ciò che ne consegue in termini di diversa puntualità ed estensione degli obblighi del titolare, nonché di minore margine di flessibilità per la disciplina nazionale.

Tra le peculiarità della direttiva (peraltro oggetto di critiche da parte del Working Party 29, precedente organismo di coordinamento delle Autorità di protezione dati), vi sono la limitazione dei diritti dell'interessato nell'ambito di procedimenti penali in base alle norme processuali interne (art. 18) e l'esclusione (necessaria) di competenza dell'Autorità di controllo rispetto ai trattamenti effettuati dalle "autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali", nonché quella (facoltativa) rispetto ai trattamenti svolti "da altre autorità giurisdizionali indipendenti nell'esercizio delle loro funzioni giurisdizionali" (art. 45, c.2, riferito in *parte qua* alle Procure, come chiarisce il Considerando 80).

Le medesime autorità possono inoltre essere esentate dall'obbligo di designazione del responsabile della protezione dati (art. 32, c.1), deputato all'osservanza delle norme della direttiva e alla tenuta dei rapporti con l'autorità di controllo.

Questo complesso di limitazioni è doverosamente volto a evitare ogni possibile interferenza di organi altri rispetto al giudiziario, la cui indipendenza è tutelata dalla stessa CDFUE in funzione della garanzia del diritto di difesa.

Nel sistema interno previgente (d.lgs. 30 giugno 2003, n. 196), del resto, il potere di controllo sui trattamenti rimesso al Garante incontrava il limite esterno del divieto di interferenza sull'esercizio della giurisdizione (cfr. anche art. 160, c.6), come espressamente rivendicato, tra l'altro, rispetto al provvedimento sulle misure di sicurezza negli uffici giudiziari (cfr. provv. n. 356 del 18 luglio 2013 e comunicato del Garante 25.9.2013).

Nel complesso, tuttavia, il testo finale delinea un bilanciamento apprezzabile tra esigenze investigative e protezione dati, rappresentato ad esempio dai principi generali cui deve conformarsi, comunque il trattamento (basato in particolare sui principi di correttezza, liceità, legalità e funzionalità del trattamento rispetto alle finalità istituzionali perseguite). Vanno garantiti segnatamente, oltre all'esattezza e qualità dei dati, anche: la differenziazione tra i dati "fondati su fatti" e quelli "fondati su valutazioni personali", una tutela rafforzata a "particolari categorie di dati" (cui ai aggiungono, rispetto alla corrispondente nozione della direttiva (CE) 95/46, anche i dati genetici, biometrici e quelli relativi all'orientamento sessuale), nonché il divieto di profilazione suscettibile di determinare discriminazioni fondate sulle stesse categorie di dati (si pensi al *racial profiling*), ulteriore rispetto alla più generale limitazione di ogni processo decisionale fondato su trattamenti automatizzati, ammissibile solo in base a espressa previsione normativa e previa adozione di garanzie adeguate per l'interessato. Importante anche il "paniere" di diritti riconosciuti all'interessato (tra cui anche quello alla limitazione del trattamento), ancorché comprimibili – oltre che ove previsto dal diritto processuale penale – anche, sebbene in misura proporzionale, in ragione di particolari esigenze investigative o di sicurezza, purché la limitazione "costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi" dell'interessato, secondo la dizione convenzionale).

Importante l'affermazione del diritto dell'interessato al risarcimento del danno derivato da trattamento illecito, di proporre reclamo all'autorità di controllo, nonché il diritto a un ricorso giurisdizionale effettivo in caso di trattamento illecito o comunque avverso una decisione della suddetta autorità ovvero avverso la sua inerzia. Come già nel regolamento, tra gli obblighi del titolare si ricomprendono anche quelli inerenti la *privacy-by-design* e *by-default*, nonché la valutazione d'impatto sulla protezione dati (che si estende anche al legislatore, tenuto a consultare l'autorità di controllo durante l'esame della normativa primaria o secondaria incidente sulla materia).

Tra le misure di sicurezza si prevede l'obbligo di notifica all'autorità di controllo (e allo stesso interessato in caso di rischi elevati non bilanciati dall'adozione di adeguate cautele) di violazioni dei dati personali.

Importanti le garanzie sancite nell'ipotesi di trasferimento di dati personali, per le finalità della direttiva, verso Paesi terzi od organizzazioni internazionali

(distinguendo i casi nei quali destinatari siano autorità competenti o meno), in base a una decisione di adeguatezza adottata dalla Commissione che tenga conto anche delle disposizioni in vigore nel settore disciplinato dalla direttiva, alla sussistenza di garanzie adeguate per la protezione dei dati (sancite in un atto giuridicamente vincolante o comunque documentate dal titolare), ovvero in ragione di deroghe specifiche funzionali alla tutela di vitali interessi individuali o collettivi. Rilevanti, infine, i poteri riconosciuti alle autorità di controllo (di natura ispettiva, prescrittiva, inibitoria, consultiva, ancorché ridotti rispetto a quelli previsti dal Regolamento) e le loro garanzie di indipendenza effettiva, nonché il ruolo attribuito anche in questo settore al Comitato europeo per la protezione dei dati.

2. Il recepimento della direttiva

La direttiva 2016/680 è stata trasposta nel nostro ordinamento con il decreto legislativo n. 51 del 2018, secondo un criterio di recepimento assai puntuale, anche in ragione dell'assenza, nella legge di delegazione, di principi e criteri direttivi specifici, ulteriori rispetto a quello inerente la cornice edittale per le fattispecie delittuose da introdurre.

Tra le scelte importanti del legislatore interno si annoverano, in particolare, le seguenti: definizione delle autorità competenti in conformità alla formulazione della direttiva ("qualsiasi autorita' pubblica dello Stato, di uno Stato membro dell'Unione europea o di uno Stato terzo competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; nonché qualsiasi altro organismo o entità incaricato dagli ordinamenti interni di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica": art. 2, c. 1, lett. g); nomina obbligatoria del responsabile della protezione dati anche per l'autorità giudiziaria nell'esercizio delle sue funzioni (art. 28, laddove la direttiva consentiva anche di prescinderne); rinvio a uno specifico d.p.r. per la previsione, nel dettaglio, dei singoli trattamenti, con la disciplina puntuale dei termini di conservazione, delle modalità di accesso, ecc. (art. 5, c. 2), fattispecie sanzionatorie amministrative modulate (quanto a condotta e criteri applicativi, non anche cornici edittali) su quelle del regolamento (art. 42), tutela del terzo coinvolto in procedimenti penali (art. 14), individuazione del Garante quale autorità di controllo nazionale unica, salvo per i trattamenti svolti dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie

del pubblico ministero (art. 37). Relativamente a questi trattamenti non è stata indicata un'autorità altra, ma si è rimesso il controllo di legittimità alla stessa sede processuale, con gli strumenti del processo, secondo la soluzione percorsa dal legislatore tedesco.

Vi è certo da dire che, nella direttiva, l'esclusione di competenza dell'autorità di protezione dati rispetto all'attività giudiziaria non equivale ad esclusione assoluta di attribuzione ad altri organi del potere di controllo, pur con modalità e garanzie tali da escludere ogni possibile violazione dei requisiti costituzionali di autonomia, soggezione esclusiva alla legge e indipendenza della magistratura da ogni altro potere. Una delle possibili soluzioni, ad esempio, avrebbe potuto essere l'attribuzione della relativa competenza al CSM, eventualmente anche integrandone la composizione (previe opportune modifiche normative) con esperti in materia o comunque prevedendo il ricorso a specifiche consulenze per questo tipo di valutazioni.

3. I dati personali contenuti in atti giudiziari, le intercettazioni e la tutela dei terzi

Una delle innovazioni più importanti introdotte dal legislatore interno[3] concerne, però, l'introduzione, all'art. 14, del diritto di "chiunque vi abbia interesse" (dunque anche del terzo) di "richiedere la rettifica, cancellazione o limitazione dei suoi dati contenuti in atti giudiziari o indagini, anche in sede processuale, con le modalità di cui all'art. 116 c.p.p.", precisandosi che "il giudice provvede con le forme dell'articolo 130 del codice di procedura penale"[4].

Vista la latitudine interpretativa della nozione di dato personale di cui all'art. 2, c. 1, lett. a) d.lgs. 51, la norma è inequivocabilmente applicabile anche ai dati contenuti alle conversazioni intercettate, sia nella forma del file audio che della relativa trascrizione. Depone in tal senso la prassi del Garante, oltre che la giurisprudenza pronunciatasi in anni di vigenza del d.lgs. 196 del 2003, che recava una nozione di dato personale appena più limitativa dell'attuale.

---

[3] E tali definite dall'allora Presidente del Garante per la protezione dei dati personali, Antonello Soro, nella Relazione annuale relativa all'anno 2018.

[4] La norma va letta in combinato disposto con il Considerando 40 della direttiva 2016/680 e con il *favo*r lì espresso per l'esercizio dei diritti da parte dell'interessato ("è opportuno predisporre modalità volte ad agevolare l'esercizio, da parte dell'interessato, dei propri diritti conformemente alle disposizioni adottate a norma della presente direttiva, compresi i meccanismi per richiedere e, se possibile, ottenere, gratuitamente, in particolare, l'accesso ai propri dati personali, la loro rettifica o cancellazione e la limitazione del trattamento").

In ragione dell'applicabilità della norma dell'art. 14, c. 1 anche ai dati contenuti nelle conversazioni captate, contenute in brogliacci o file audio, essa sancisce in capo non solo alle parti processuali ma anche al terzo, il diritto di ottenere, con le forme particolarmente agili delle procedure di cui agli artt. 116 e 130 c.p.p., la rettifica, cancellazione o limitazione dei dati che lo riguardano.

Tale interpretazione è "suffragata", oltre che dal Considerando 47 della direttiva 2016/680, anche dalla interpretazione "ufficiale" fornita dal Presidente del Garante per la protezione dei dati personali, nell'ambito della Relazione 2018, secondo cui "*È significativa, ad esempio, la previsione del diritto della persona (a prescindere dalla posizione processuale, includendovi anche il terzo estraneo alle indagini) di richiedere, con una procedura particolarmente agile, la cancellazione o rettifica dei propri dati illegittimamente trattati in ambito giudiziario penale. Norma, questa, che potrebbe risultare particolarmente utile anche rispetto alle conversazioni intercettate*". Analoga posizione è stata rappresentata nell'ambito del Convegno *La rivoluzione mancata. A proposito di riforma della disciplina delle intercettazioni,* (13 novembre 2018, disponibile su http://www.radioradicale.it/scheda/557504/) in cui si rilevava come la norma coprisse, sostanzialmente, alcune delle lacune derivanti dal differimento (allora vigente) dell'applicabilità dell'art. 2 del d.lgs. 29 dicembre 2017, n. 216, quale suo equivalente funzionale[5].

La richiesta va rivolta al titolare del trattamento (cfr. artt. 12-15 direttiva 2016/680, nonché artt. 10, 11 e 12 dello stesso d.lgs. 51, richiamati dall'art. 14) che, secondo la fase processuale, dovrà essere individuato con il regolamento attuativo di cui all'art. 5, c. 2, d.lgs. 51. In ogni caso, il giudice (che potrebbe comunque ritenersi competente a decidere, per ragioni di terzietà, anche laddove il titolare per fase processuale sia il Pubblico Ministero) sarà tenuto a osservare le forme della procedura per la correzione degli errori materiali.

Quanto al contenuto delle richieste suscettibili di proposizione in questa sede da parte dell'interessato, la norma menziona anzitutto il diritto di cancellazione, da esercitarsi secondo i criteri generali di cui all'art. 269, c. 2, c.p.p. (ove riguardi le intercettazioni) e, dunque, in relazione a dati non necessari a fini probatori o investigativi, dal momento che tale assenza di necessità renderebbe per ciò solo la conservazione di dati personali (*a fortiori* se di soggetti terzi rispetto alle indagini) illegittima per violazione dei principi di finalità, proporzionalità, non eccedenza di cui all'art. 3 d.lgs. 51 (salvo volersi riferire la nozione di necessità a procedimenti diversi, nei quali le conversazioni potrebbero rifluire *ex* art. 270 c.p.p.).

---

[5] V. anche S. Signorato, *L'archivio delle intercettazioni. La custodia del materiale e la marcia verso la digitalizzazione delle intercettazioni,* in *Legislazione pen.*, 2020, 79 ss.

Qualora la cancellazione debba essere rigettata per esigenze di conservazione probatoria, l'interessato può però chiedere la limitazione del trattamento (v. *infra*), che consiste essenzialmente nel trasferire i dati "ad altro sistema di archiviazione" o nel rendere inaccessibili i dati stessi.

La rettifica concerne invece la correzione di dati inesatti: "*Una persona fisica dovrebbe avere il diritto di ottenere la rettifica di dati personali inesatti che la riguardano, in particolare se relativi a fatti, e il diritto alla cancellazione quando il trattamento di tali dati viola la presente direttiva. Il diritto di rettifica, tuttavia, non dovrebbe avere effetti, ad esempio, sul contenuto di una prova testimoniale*". (cfr. C 47 della direttiva)

La limitazione riguarda, per altro verso, i casi nei quali la legittimità del trattamento del dato sia in discussione ma non possa accertarsi, almeno nel momento considerato, l'effettiva fondatezza della richiesta o, comunque, sussistano esigenze di conservazione dei dati a fini probatori (cfr. Considerando 47 della direttiva).

Il Considerando 47 precisa inoltre che le rettifiche, al pari delle cancellazioni e limitazioni di dati personali "dovrebbero essere comunicate ai destinatari a cui tali dati sono stati comunicati e alle autorità competenti da cui i dati inesatti provengono. I titolari del trattamento dovrebbero inoltre astenersi dal diffondere ulteriormente tali dati".

La limitazione del trattamento, dunque, potrebbe essere una valida misura (da attuare anche, in ipotesi, con la custodia nel luogo protetto previsto per le intercettazioni illegali *ex* art. 240, c. 2, c.p.p., ovvero nell'archivio riservato) da attuare rispetto a dati personali contenuti, ad esempio, in conversazioni captate in attesa del vaglio effettivo di rilevanza.

Naturalmente, poi, venuta meno la concreta possibilità di un'utilizzazione processuale, le intercettazioni oggetto di limitazione dovrebbero essere cancellate (con le forme dell'art. 269, c. 2, c.p.p.) in ottemperanza ai principi di non eccedenza del trattamento che si applicano, appunto, anche agli atti giudiziari *ex* art. 3 d.lgs. 51 del 2018.

Si tratta di una norma che ben potrebbe essere valorizzata a fini di tutela, appunto, dei soggetti a qualunque titolo coinvolti nelle intercettazioni., laddove non abbiano sortito effetto i criteri di "sobrietà contenutistica" e minimizzazione selettiva imposti, in sede di trascrizione, dalla disciplina vigente, come riformata per effetto della successione tra le leggi il d.lgs. 216 del 2017 e il dl. n. 161 del 2019, convertito, con modificazioni, dalla legge n. 7 del 2020.

Al fine di garantire la tutela effettiva dei terzi, tuttavia, sarebbe opportuno prevedere un onere informativo a carico del Pubblico ministero – come era previsto dall'art. 268-*sexies* c.p.p. di cui l'art. 10 del d.d.l. Mastella di riforma delle intercettazioni della XV legislatura (AS 1512), prospettava l'introduzione – per evitare che il soggetto apprenda dell'esistenza, in atti processualidi proprie

conversazioni, direttamente dalla stampa, quando ormai l'intervento ablativo sarebbe tardivo.

In alternativa (ove tale onere informativo venisse ritenuto eccessivamente gravoso, soprattutto a fronte di una pluralità di soggetti da avvisare), si potrebbe riconoscere al terzo il diritto di chiedere preliminarmente conferma dell'esistenza di intercettazioni che lo coinvolgano e, quindi, previo ascolto delle registrazioni stesse, di attivare la procedura di distruzione di cui all'art. 269 cpp[6] ovvero, in caso di richieste più articolate, di esercitare i propri diritti alla limitazione o (più raramente) rettificazione dei dati.

In tal modo, tramite la connessione procedimentale tra il nuovo diritto di cui all'art. 14 d.lgs. 51 e l'istituto della distruzione di cui all'art. 269 c.p.p. (testualmente rivolto agli «interessati»), ai terzi i cui dati siano occasionalmente captati in sede intercettativa potrebbe essere accordata una tutela effettiva, forse persino più di quanto si sia ipotizzato in, pur ampie e valide, ipotesi di riforma della disciplina delle intercettazioni. Si tratta di studiare, ancora, le modalità più opportune e meno gravose per gli uffici giudiziari, ma idonee a garantire la tutela effettiva della *privacy* delle parti e dei terzi.

[6] S. Renzetti, *Una riforma (radicale?) per tornare allo spirito originario della legge: la nuova disciplina acquisitiva delle intercettazioni tra legalità, diritto vivente e soft law, in Legislazione pen.*, 2018, 1 ss.

Filippo Donati

La giustizia e le nuove tecnologie

Sommario: 1. – Premessa. – 2. Le potenzialità dei software "predittivi". – 3. L'affidabilità dei sistemi di IA. – 4. Limiti all'impiego dell'IA nel campo della giustizia. – 5. Possibili impieghi dell'IA nel campo della giustizia. – 6. Considerazioni conclusive.

1. Premessa

Nella riunione (*online*) svolta il 9 ottobre 2020 tra i Ministri della giustizia dell'Unione europea[1], sono stati evidenziati i vantaggi derivanti della digitalizzazione e dall'applicazione dei nuovi sistemi di intelligenza artificiale (IA) alla giustizia. La Commissione europea, nella comunicazione "*digitalization of justice in the European Union. A toolbox of opportunities*" dello scorso 2 dicembre 2020, ha proposto un ambizioso piano di azione per promuovere la digitalizzazione dei sistemi di giustizia nazionali e l'impiego di piattaforme digitali per gli scambi transfrontalieri di documenti e informazioni. La Commissione ha, inoltre, promesso un supporto allo sviluppo ed all'impiego dell'IA, sottolineando i vantaggi che da questa nuova tecnologia possono discendere per un miglioramento della qualità e dell'efficienza della funzione giudiziale.

Esiste, dunque, una diffusa consapevolezza, al livello europeo, sulla esigenza di non lasciarsi sfuggire le potenzialità che l'IA offre anche per il settore giustizia.

---

[1] Richiamata in https://www.consilium.europa.eu/it/meetings/jha/2020/10/09/#. Christine Lambrecht, ministra federale tedesca della Giustizia e della tutela dei consumatori, ha sottolineato che "la digitalizzazione del sistema giudiziario è un'enorme opportunità, che possiamo sfruttare a nostro vantaggio in questo periodo di pandemia. La digitalizzazione può aiutarci a far sì che tutti i cittadini abbiano accesso in qualsiasi momento a tribunali indipendenti e può rendere più efficienti le nostre procedure. L'intelligenza artificiale, ad esempio, può assistere i giudici nel loro lavoro e promuovere la comparabilità e la qualità delle decisioni. I sistemi di IA devono essere trasparenti, completi, sicuri, sottoposti a revisione e non discriminatori". La Presidente ha peraltro evidenziato che "le decisioni giudiziarie non possono essere completamente automatizzate. La decisione finale deve sempre spettare a un giudice".

Qui di seguito svolgerò alcune riflessioni sulle opportunità e i rischi dell'impiego dell'IA come strumento a servizio della giustizia[2].

2. Le potenzialità dei *software* "predittivi"

Nel 2017 è stata organizzata una singolare gara, denominata *Case Crunch Lawyer Challenge*. La gara, che avuto un certo rilievo anche nei media[3], ha messo a confronto 100 "*top lawyers*" della *City* di Londra con un sistema di IA.

La gara aveva ad oggetto la previsione di controversie, risolte dal *Financial Ombudsman*, relative a particolari clausole contrattuali, denominate PPI (*payment protection insurance*), volte a garantire i consumatori contro rischi relativi ad eventi (morte, invalidità, disoccupazione ecc.) che potrebbero rendere difficile la restituzione del finanziamento. Queste clausole hanno dato origine ad un vasto contenzioso in Inghilterra, perché si sono rivelate spesso troppo costose e non adeguate ad offrire una effettiva protezione per i consumatori.

Gli organizzatori[4] hanno fornito ai concorrenti i dati di fatto relativi alle controversie, senza però comunicare, né agli umani né al sistema di IA, la decisione finale assunta al riguardo dal *Financial Ombudsman*.

I partecipanti hanno analizzato 775 casi. Il *software* ha vinto a mani basse, fornendo risposte con un tasso di esattezza dell'86.6%, di molto superiore al punteggio di 66.3% raggiunto dagli avvocati. Senz'altro un trionfo, è stato osservato, per una piccola *start-up*. In effetti, il sistema di IA impiegato nella gara era stato sviluppato non da una multinazionale, ma da una piccola impresa fondata da quattro ex studenti di *Cambridge*.

In definitiva, la macchina si è dimostrata capace di fornire risposte più accurate, più rapide e, verosimilmente, a costi più bassi di quanto non siano riusciti a fare numerosi avvocati di fama.

Altri esperimenti di giustizia predittiva hanno offerto risultati sorprendentemente positivi. Nel 2016 è stato sviluppato, presso l'*University college of London,* un algoritmo in grado offrire previsioni fortemente attendibili sul possibile esito di controversie dinanzi alla Corte europea dei diritti dell'uomo. L'algoritmo, prendendo in esame la giurisprudenza della Corte (584 decisioni), si è rivelato idoneo a valutare la violazione o meno degli articoli 3, 6 e 8 della Convenzione in nuovi

---

[2] In argomento cfr. anche, eventualmente, F. Donati, *Intelligenza artificiale e giustizia*, in *Rivista AIC*, n. 1/2020, 515 ss.

[3] R. Cellan-Jones, *The robot lawyers are here – and they're winning*, *BBC News*, 10/10/2020.

[4] Felix Steffek, un docente dell'Università di *Cambridge*, e Ian Dodd, un dirigente di *Premonition Analytics*, una società che gestisce uno dei più sviluppati database nel campo legale.

casi concreti posti all'attenzione della Corte, con un margine di successo fino al 79%[5]. Sono stati inoltre realizzati, più recentemente, sistemi per prevedere l'esito di controversie dinanzi alla Corte suprema degli Stati Uniti[6], la Corte suprema francese[7], e ancora la Corte europea dei diritti dell'uomo[8], che hanno offerto un tasso di accuratezza compreso tra il 70% e il 96%. Una media, pertanto, superiore all'80%.

Non è quindi azzardato prevedere che, in futuro, professionisti, privati cittadini e imprese potrebbero essere sempre più indotti ad utilizzare sistemi del genere per orientare le proprie scelte quando si tratta, ad esempio, di decidere se avviare o meno una determinata controversia ovvero accettare una proposta transattiva. Sistemi di IA, del resto, sono ormai da tempo in uso presso grandi compagnie di assicurazioni e studi legali.

L'utilizzabilità di sistemi di IA nel campo della giustizia richiede, tuttavia, il superamento di problemi di carattere tecnico e giuridico.

3. L'affidabilità dei sistemi di IA

La principale caratteristica dei nuovi sistemi di IA è quella di operare in via autonoma. Tali sistemi si basano, infatti, su meccanismi di autoapprendimento o di "*machine learning*". A differenza dei tradizionali computer, il *software* alla base di tali sistemi non è costituito da una serie di regole fisse e predeterminate, ma da regole che variano continuamente in base ad analisi statistiche di grandi quantità di dati.

Vari sono i fattori che possono incidere sull'attendibilità di un sistema di IA.

In primo luogo, il buon funzionamento del sistema può essere compromesso da problemi di "apprendimento", ovvero dalla gestione non corretta dei dati presi

---

[5] Cfr. N. Aletras – D. Tsarapatsanis – D. Preotiuc-Pietro – V. Lampos, *Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective*, in *PeerJ Computer Science* 2:e93, in *https://doi.org/10.7717/peerj-cs.93*. Cfr. anche M. Medvedeva – M. Vols – M. Wieling, *Using machine learning to predict decisions of the European Court of Human Rights*, in *Artificial Intelligence Law*, 28(2) 2019, 237-266, i quali hanno dimostrato la possibilità, attraverso tecniche di analisi del linguaggio, di predire l'esito di casi dinanzi alla Corte EDU con un'accuratezza di circa il 75%.

[6] Cfr. D.M. Katz – M.J. Bommarito – J. Blackman, *A General Approach for Predicting the Behavior of the Supreme Court of the United States*, in *PloS ONE* 12(4)2017.

[7] Cfr. O.M. Sulea – M. Zampieri – M. Vela – J. Vangenabith, *Predicting the law area and decisions of French Supreme Court cases,* in *RANLP* (4) 2017.

[8] Cfr. I. Chalkids – I. Androutsopoulus – N. Aletras, *Neural Legal Judgment in English,* in *Association for Computational Linguistics*, 2019, 4317 ss.

in considerazione nella fase in cui il *software* elabora i propri modelli decisori (i cosiddetti "*training data*"). Se questi dati non sono stati raccolti correttamente oppure contengono errori, l'attendibilità dei risultati offerti dal sistema ne risulta inevitabilmente compromessa.

In secondo luogo, vi possono essere errori nella progettazione del *software*.

È nota la vicenda relativa al sistema COMPAS[9], un programma di IA progettato per calcolare il rischio di recidiva e la pericolosità sociale delle persone. La Corte suprema del *Wisconsin*, nel caso *State c. Loomis*[10], ha applicato una pesante misura detentiva nei confronti del sig. Loomis che, secondo i dati forniti dal sistema, presentava una forte tendenza alla recidiva. Successivamente alla sentenza è stato però dimostrato che, il sistema COMPAS produce effetti discriminatori perché tende ad attribuire un rischio di recidiva maggiore a determinate persone in relazione al colore della pelle ed all'ambiente sociale di riferimento, fornendo, in molti casi, inaccettabili indicazioni che conducono a scelte "razziste".

In effetti, come sottolineato dalla Commissione europea nella comunicazione sulla digitalizzazione della giustizia in Europa, accanto agli innegabili vantaggi che l'impiego di sistemi di IA potrebbe apportare nel campo della giustizia, vi sono rischi non trascurabili da prendere in attenta considerazione. Anche il recente libro bianco sull'intelligenza artificiale[11], evidenzia una serie di problemi, come ad esempio la non trasparenza del processo decisionale dei sistemi di IA, la possibilità di discriminazioni dovute a pregiudizi o difetti del sistema, i rischi inerenti al trattamento di enormi moli di dati personali.

Non è tuttavia azzardato prevedere che lo sviluppo della ricerca e l'evoluzione della tecnologia consentiranno in futuro di mitigare i rischi richiamati, rendendo sempre più affidabile l'impiego di sistemi di IA.

Gli errori dovuti ai difetti dei "*training data*" sono quelli che destano minori preoccupazioni, perchè possono essere mitigati attraverso la creazione di *database* sempre più completi ed accurati. Anche gli algoritmi possono essere migliorati per limitare malfunzionamenti del sistema.

---

[9] *Correctional Offenders Managment Profilying for Alternative Sanctions*. COMPAS è un *software* che valuta il rischio di recidivismo attraverso un'analisi statistica basata su informazioni ottenute dall'imputato attraverso un'intervista e sui dati giudiziari relativi all'imputato, valutati sulla base di dati statistici relativi a campioni di popolazione. Il *software* è commercializzato da Northpointe inc. che ne detiene i diritti e le licenze commerciali.

[10] 881 N.W.2nd 749 (Wis. 2016).

[11] Commissione europea, *Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, Bruxelles, 19.2.2020 COM(2020) 65 finale.

L'imposizione di oneri di trasparenza per le decisioni algoritmiche che incidono sui diritti della persona, inoltre, potrebbe consentire di meglio controllare il funzionamento e l'attendibilità dei sistemi di IA, in modo da garantire una tutela giudiziaria effettiva delle situazioni giuridiche in ipotesi lese. Nell'ambito del procedimento amministrativo, ad esempio, il Consiglio di Stato ha chiarito che le decisioni automatizzate debbono essere "trasparenti". L'amministrazione, in altre parole, deve permettere agli interessati di conoscere le regole sottese all'algoritmo e le sue principali caratteristiche, e la "decisione algoritmica" deve poter essere sottoposta a controllo giurisdizionale. Analoga trasparenza è necessaria, a maggior ragione, quando i sistemi di IA vengano impiegati a supporto della funzione giurisdizionale.

Laddove le caratteristiche del sistema rendessero difficile o impossibile ottenere adeguate indicazioni sulla "logica" impiegata per ottenere determinate decisioni, resterebbe comunque la possibilità di sottoporre il funzionamento del sistema ad un controllo "contro-fattuale". Così, ad esempio, per valutare se l'impiego di un sistema algoritmico di selezione del personale conduce a discriminazioni di genere, se ne potrebbe testare il comportamento quando due candidati di sesso diverso presentano *curricula* identici. Se, all'esito della prova, il sistema dovesse scegliere uno dei due candidati, saremmo in presenza di un indice di non attendibilità dello stesso.

In futuro, sarà necessario introdurre sistemi di certificazione e di controllo sull'affidabilità dei sistemi di IA. In questa prospettiva, il Libro bianco sull'intelligenza artificiale propone di affidare ad apposite autorità il compito di verificare l'affidabilità dei sistemi di IA, la sicurezza degli stessi nonché l'idoneità a garantire il rispetto dei diritti fondamentali. I sistemi che evidenziassero errori o discriminazioni non potrebbero, ovviamente, essere suscettibili di impiego.

4. Limiti all'impiego dell'IA nel campo della giustizia

Anche se gli ostacoli di natura tecnica venissero superati, rimarrebbero ostacoli di natura giuridica a certi tipi di utilizzo dell'IA nel campo della giustizia.

La sostituzione di giudici con robot, ad esempio, non è consentita dalla nostra Costituzione.

La previsione di forme obbligatorie di soluzione automatizzata delle liti violerebbe numerose disposizioni costituzionali: l'art. 102, che affida l'esercizio della funzione giurisdizionale a magistrati istituiti e regolati dalle norme sull'ordinamento giudiziario, l'art. 111, che impone lo svolgimento dei processi davanti a un giudice terzo e imparziale, l'art. 101, che vincola i giudici al solo rispetto della legge (con ciò implicitamente escludendo vincoli derivanti dall'esito di

procedure algoritmiche), l'art. 25, che garantisce il diritto al un "giudice naturale precostituito per legge.

La sostituzione del giudice con meccanismi automatizzati di soluzione delle controversie, inoltre, rischierebbe di compromettere le garanzie offerte dalla nostra Carta costituzionale attinenti alla giurisdizione, quali l'effettività e la pienezza del diritto alla difesa delle parti, la qualità della decisione giurisdizionale, la capacità del giudice di far emergere la peculiarità dei fatti su cui orientare la decisione e, infine, l'obbligo di motivazione.

In effetti, i sistemi di giustizia predittiva non motivano. Un sistema di IA offre la soluzione del caso concreto senza dare quella spiegazione che, invece, siamo soliti ricevere da un giudice o da qualsiasi altro soggetto chiamato a dirimere una controversia. Non è però possibile fare a meno della motivazione giudiziale della decisione, che sostanzia il cuore delle garanzie costituzionali del processo e della stessa imparzialità dell'organo giudicante.

I sistemi di giustizia predittiva potrebbero peraltro trovare uno spazio di utilizzazione nelle procedure alternative di soluzione delle controversie, in particolare quelle che riguardano i cosiddetti *small-claims*, ovvero le questioni di valore economico così basso che difficilmente verrebbero fatti valere dinanzi a un giudice. In casi del genere, i sistemi di IA potrebbero fornire un ausilio per il raggiungimento di accordi transattivi, fornendo così forme di tutela alternative, che ovviamente non possono escludere o limitare il diritto alla tutela giurisdizionale.

5. Possibili impieghi dell'IA nel campo della giustizia

Nonostante il limite richiamato sopra, grandi sono le potenzialità derivanti dall'impiego dei moderni sistemi di IA nel campo della giustizia.

Già oggi sistemi di IA vengono impiegati dalle grandi *law firms* per la ricerca di informazioni o l'analisi di testi giuridici, specie nell'ambito di quelle ampie operazioni di *due diligence* che richiedono l'esame di migliaia di documenti. In tal modo, la macchina finisce per sostituire il lavoro usualmente affidato ai giovani avvocati.

L'impiego dei nuovi sistemi di IA potrebbe, inoltre, rivelarsi utile per la ricerca dei precedenti. Essi potrebbero, in altre parole, fornire nuovi e più potenti motori di ricerca.

Strumenti del genere servirebbero agli avvocati e alle parti per valutare la probabilità di successo o di insuccesso di un determinato caso, per decidere se impugnare o meno una determinata decisione, o anche per valutare i termini di un eventuale accordo transattivo.

Per quanto riguarda gli organi giudiziari, pur non vigendo nel nostro sistema l'obbligo di rispettare il precedente, esiste tuttavia l'esigenza di garantire l'affidamento del cittadino nella certezza del diritto. L'uniforme applicazione del diritto è del resto indispensabile per garantire il rispetto del principio di eguaglianza dei cittadini di fronte alla legge. In questa prospettiva, il nuovo art. 374 c.p.c., come modificato dal d.lgs. n. 40 del 2006, obbliga le sezioni semplici della Corte di Cassazione, quando non condividono un precedente delle Sezioni Unite, a rimettere a queste ultime, con ordinanza motivata, la decisione del ricorso. Analogamente, l'art. 99, comma 3, del codice del processo amministrativo stabilisce che "se la sezione cui è assegnato il ricorso ritiene di non condividere un principio di diritto enunciato dall'adunanza plenaria, rimette a quest'ultima, con ordinanza motivata, la decisione del ricorso", Una esatta e tempestiva conoscibilità dei precedenti potrebbe inoltre rivelarsi utile in sede di applicazione dei nuovi meccanismi di "filtro" in Cassazione (art. 360-*bis* c.p.c.) e in appello (art. 348-*bis* c.p.c.), nonché, più in generale, per supportare le decisioni di volta in volta da adottare.

I sistemi di IA potrebbero, inoltre, offrire un ausilio in ogni caso in cui si tratta di effettuare valutazioni tecniche volte alla determinazione di importi monetari nell'ambito di giudizi civili come, ad esempio, la determinazione dell'indennità dovuta in caso di licenziamento o l'importo dell'assegno divorzile o, più in generale, in tutti i casi in cui la valutazione si fonda su elementi numerici e su valutazioni tecnico-scientifiche, come ad esempio nel computo delle percentuali sull'invalidità civile. Ancora, l'IA potrebbe offrire aiuti nei servizi di traduzione, di dettatura automatica, o anche per la predisposizione e la correzione delle bozze dei provvedimenti.

6. Considerazioni conclusive

Si va diffondendo, in Europa, la consapevolezza dell'utilità dell'impiego delle nuove tecnologie informatiche a servizio della giustizia. Nei documenti elaborati dalla Commissione e da altre istituzioni dell'Unione europea e del Consiglio d'Europa, si dà ormai per scontata l'utilità dell'impiego dei sistemi di IA anche nel campo della giustizia e si punta, pertanto, a garantire un utilizzo di questi sistemi rispettoso dei diritti fondamentali.

La Commissione ha istituito un gruppo di esperti ad alto livello che, nell'aprile 2019, ha pubblicato orientamenti per un'IA affidabile[12]. In considerazione della "crescente importanza dell'IA nella moderna società" e dei "benefici attesi una

[12] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top.

volta che le sue potenzialità verranno impiegate anche a servizio dell'efficienza e della qualità della giustizia", la Commissione europea per l'efficacia della giustizia (CEPEJ), istituita dal Comitato dei ministri del Consiglio d'Europa, ha adottato la Carta etica europea per l'uso dell'IA nei sistemi giudiziari[13].

La Carta etica è il primo documento volto a stabilire criteri volti ad orientare le modalità di sviluppo e di impiego di sistemi di IA a supporto delle decisioni giudiziali. La Carta etica indica che l'IA, se utilizzata come strumento non di sostituzione, ma di ausilio del giudice, può, in determinate circostanze, favorire la prevedibilità nell'applicazione della legge e l'uniformità degli orientamenti giurisprudenziali.

L'impiego dell'IA a servizio della giustizia, però, deve garantire il rispetto dei limiti imposti dal nostro modello costituzionale e dai principi etici che rilevano in materia. L'Agenzia europea dei diritti fondamentali ha recentemente pubblicato un ampio studio sull'incidenza dell'impiego dell'IA sui diritti umani.

In definitiva, nuovi sistemi di IA, se utilizzati in modo tale da garantire il rispetto dei diritti fondamentali, potranno contribuire ad un miglioramento complessivo della qualità e dell'efficienza della nostra giustizia.

[13] *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment*, adottata dalla CEPEJ nella 31ª assemblea generale (Strasburgo, 3-4 Dicembre 2018, CEPEJ(2018)14.

Giovanni Canzio

Intelligenza artificiale e processo penale[1]

Sommario: 1. Un perimetro definitorio. – 2. L'ambiente. – 3. *Calculemus!* – 4. Giustizia predittiva e standard "debole" dell'IA. – 5. *Digital Evidence* e processo penale. – 6. Il contraddittorio "per" la prova e l'art. 189 c.p.p. – 7. Qualche conclusione provvisoria.

1. Un perimetro definitorio

L'intelligenza artificiale applicata al settore della giurisdizione (*Legal AI*) può definirsi un sistema digitale che, con specifico riguardo all'ambiente della giustizia, acquisisce, ordina e rielabora una enorme quantità di informazioni (*Big Data*), di tipo giudiziario o giurisprudenziale, al fine di identificare la soluzione ottimale della questione posta. In pratica: un sistema tecnologico che simula il processo cognitivo e decisorio dell'uomo e che, sulla base di calcoli algoritmici di tipo probabilistico, frutto di processi di apprendimento, auto-apprendimento (*Machine-Learning*) e ragionamento, è in grado di formulare la previsione della soluzione corretta (*giustizia predittiva*) o addirittura la stessa decisione.

Sono queste le caratteristiche del modello "*forte*" dell'intelligenza artificiale, che, attraverso complesse operazioni di *input* e *output* dei dati, postula l'automazione del processo decisionale (*machina sapiens*) in luogo degli attori tradizionali della giurisdizione.

Orbene, non può seriamente dubitarsi che, a fronte della crisi di certezza, calcolabilità, prevedibilità, uniformità, trasparenza e celerità delle tradizionali procedure della giurisdizione, la forza espansiva di un tale sistema, che promette di offrire un'efficiente e pronta risposta alla domanda di giustizia in termini di regola tecnico-scientifica, perciò neutra, oggettiva e deresponsabilizzante per il decisore, comporti il rischio di un mutamento di paradigma del dire e fare il diritto nel XXI secolo, incidendo pesantemente anche sull'etica del giudizio.

---

[1] Testo riveduto e ampliato degli interventi svolti in occasione dei Webinar organizzati sullo stesso tema, rispettivamente, dalla Fondazione Leonardo – Civiltà delle Macchine il 20/10/2020, dalla SSM il 18/1/2021 e dal DSG dell'Università di Firenze il 22/1/2021.

2. L'ambiente

Con riguardo alla perimetrazione dell'ambiente della giurisdizione penale, come luogo del potenziale intervento dei sistemi di intelligenza artificiale, occorre partire dalla descrizione dello statuto epistemologico e costituzionale del processo moderno, la cui funzione cognitiva e aletica s'ispira al modello occidentale del razionalismo critico e che fa perno sul più debole "*paradigma indiziario o divinatorio*" rispetto al più robusto "*paradigma galileiano o scientifico*"[2]. Il processo penale s'innerva, infatti, intorno ai concetti di ipotesi e fatti, indizi e prove, contraddittorio, verità e dubbio, conferma e falsificazione dell'ipotesi, giustificazione razionale della decisione, controllo impugnatorio della motivazione. Da un principio d'ipotesi, attraverso le indagini condotte sulla base di segni e tracce, fino alla scoperta della verità si snoda il percorso cognitivo e decisorio del processo penale. Di qui, l'ormai acquisita consapevolezza della valenza soltanto probabilistica del giudizio di conferma dell'enunciato di partenza, in funzione dell'accertamento dell'ottimale corrispondenza, verosimiglianza, plausibilità dell'ipotesi rispetto al fatto realmente accaduto nel passato (*lost facts*). Il paradigma indiziario postula, cioè, non la certezza o verità materiale e assoluta, ma l'alta credibilità razionale della soluzione decisoria di conferma dell'enunciato di accusa, in termini di alta e qualificata probabilità.

Nel *trial by probabilities*, pur prendendo le mosse dalla quantità e dalla qualità delle informazioni disponibili, la neutralità del ragionamento inferenziale e delle stime probabilistiche, che nella pratica giudiziaria sono alla base dell'opera logica di valutazione delle prove e della decisione, non sono dunque immuni dal rischio di distorsioni ed errori cognitivi, a causa della razionalità limitata e dei limiti computazionali di funzionamento della mente umana ("*anche i giudici sono esseri umani*")[3].

---

[2] C. Ginzburg, *Spie. Radici di un paradigma indiziario*, in *Crisi della ragione*, Einaudi, 1979.

[3] Khaneman-Slovic-Tversky, *Judgement under Uncertainty, Heuristics and Biases*, Cambridge, 1982; D. Khaneman, *Pensieri lenti e veloci,* Milano, 2012; P. Rumiati, *Saper decidere. Intuizioni, ragioni, impulsività*, Bologna, 2020; P. Rumiati – C. Bona, *Dalla testimonianza alla sentenza. Il giudizio tra mente e cervello*, Bologna, 2019; G. Cevolani – V. Crupi, *Come ragionano i giudici: razionalità, euristiche e illusioni cognitive*, in *disCrimen,* 22 ottobre 2018; A. Forza – G. Menegon – P. Rumiati, *Il giudice emotivo. La decisione tra ragione ed emozione*, Bologna, 2017; G. Insolera, *Legge, ragione ed emozione nella giustizia penale*, in *disCrimen*, 14 febbraio 2020. A proposito dell'opera del giudice-interprete, merita di essere riportato il pensiero tagliente di C. Beccaria, *Dei delitti e delle pene*, a cura di F. Venturi, Torino, 2007, § 4, Interpretazione delle Leggi: « *... Lo spirito della legge sarebbe dunque il risultato di una buona o cattiva logica di un giudice, di una facile o malsana digestione; dipenderebbe dalla violenza delle sue passioni, dalla debolezza di chi soffre, dalle relazioni del giudice coll'offeso, e da tutte quelle minute forze che cangiano le apparenze di ogni oggetto nell'animo*

Per ridimensionare o almeno ridurre al minimo l'impatto negativo sull'esercizio della giurisdizione penale dei *biases* cognitivi, l'ordinamento giuridico appresta una fitta rete di regole epistemologiche e di legalità, sia del procedere che del ragionamento probatorio, mirate al controllo del buon funzionamento e dell'efficacia di quel giudizio.

Esse s'ispirano innanzitutto ai metavalori costituzionali che, a fronte delle difficoltà pratiche di ricostruzione del fatto e della strutturale incertezza del giudizio, disciplinano il "*giusto processo*": la presunzione di innocenza dell'imputato e l'onere della prova a carico dell'accusa; il principio del contraddittorio come metodo dialettico di verifica delle prove e di ricerca della verità; il giudizio conclusivo di conferma o falsificazione dell'ipotesi, nel contesto di una motivazione e alla stregua del criterio dell'"*al di là di ogni ragionevole dubbio*"; il controllo impugnatorio di legalità e logicità della giustificazione.

Il codice di rito penale, a sua volta, recependo a grandi linee il sistema accusatorio, traccia i percorsi di verità che guidano il ragionamento probatorio e la decisione giudiziale, sulla base di regole logico-epistemiche (artt. 187, 192, comma 1, 546, comma 1 lett. e, 606 lett. e) che disegnano un vero e proprio modello di motivazione in fatto della sentenza penale.

In estrema sintesi: in ossequio al modello tradizionale del razionalismo critico, la legge (art. 101, comma 2 Cost.) e la motivazione (art. 111, comma 6 Cost.) costituiscono il duplice *anchorage* costituzionale della razionalità del giudicare e le solide fonti di legittimazione della giurisdizione e dei giudici[4].

3. *Calculemus!*

Nel vedere due filosofi che si affrontano in una *disputatio*, G.W. von Leibniz invita entrambi a "*sumere calamos et abacos*", le tavolette di calcolo, e attraverso la formalizzazione del linguaggio e dei concetti, a convertirsi in "*calculatores*" per risolvere correttamente la controversia. Al "*Calculemus*" di Leibniz (1684) rispose negli anni '30 del secolo scorso B.N. Cardoso, giudice della Corte Suprema USA, sostenendo viceversa che "*ancora non è stata scritta la tavola dei logaritmi per la formula di giustizia*".

---

fluttuante dell'uomo. Quindi veggiamo la sorte di un cittadino cambiare spesse volte nel passaggio che fa a diversi tribunali e le vite de' miserabili essere la vittima dei falsi raziocinii o dell'attuale fermento degli umori d'un giudice che prende per legittima interpretazione il vago risultato di tutta quella confusa serie di nozioni che gli muove la mente...».

[4] Cfr., volendo, G. Canzio, *La motivazione della sentenza e la prova scientifica:* "reasoning by probabilities", in G. Canzio – L. Luparia (a cura di), *Prova scientifica e processo penale*, Milano, 2018, 3 ss.

Da almeno due decenni si assiste tuttavia alla decisa irruzione nel processo penale della prova tecnologica e scientifica, e, ancora più di recente, al progressivo ingresso di varie e inedite forme di intelligenza artificiale.

Va emergendo il fenomeno dell'utilizzo da parte delle Corti statunitensi (il *leading case* è identificato in *Wisconsin S.C., State v. Loomis*[5]), di tecniche informatiche per misurare il rischio di recidivanza del condannato, ai fini della determinazione dell'entità della pena o di una misura alternativa alla detenzione, nella fase del *sentencing* o dell'esecuzione, della sospensione condizionale o della libertà su cauzione. Per il giurista continentale appare agevole il rinvio concettuale agli istituti delle misure cautelari, di prevenzione o di sicurezza, che vengono applicate sulla base di una prognosi ovvero di un giudizio probabilistico allo stato degli atti.

L'apprezzamento di merito del giudicante in ordine alla propensione dell'imputato a ripetere il delitto non trova la soluzione in un criterio metodologico di accertamento del fatto e neppure in una puntuale prescrizione della legge, ma viene affidato a un algoritmo predittivo[6] di valutazione del rischio (*Risk Assessment Tools*), elaborato da un *software* giudiziario (*COMPAS*: acronimo di *Correctional Offender Management Profiling for Alternative Sanctions*), brevettato e prodotto dalla società privata *Northpointe*, che vanta il segreto industriale su codice sorgente, database e tecniche di elaborazione dei dati. L'interessato deve rispondere a un questionario formato da ben 137 domande; alla luce delle risposte fornite viene attribuito un punteggio di pericolosità da 1 a 10, sulla base di indici di riferimento ritenuti significativi, quali i dati circostanziali del caso concreto, le condizioni soggettive, familiari, sociali e di *status*, i precedenti penali e le pendenze giudiziarie ecc.

Sono evidenti i risultati pratici, in termini di risparmio di tempi e costi, di semplificazione delle procedure e di tendenziale calcolabilità e uniformità delle decisioni (oltre che di ridotta responsabilità del giudicante, con l'inevitabile effetto di conformismo e sclerotizzazione del formante giurisprudenziale), conseguiti dall'impiego del modello matematico-statistico nell'esercizio di quella che viene definita "*giustizia predittiva*".

Sicché, neppure le cautele e i *warning* delle Corti o lo scetticismo dei giuristi, quanto al rispetto delle garanzie del "*due process*", nella raccolta delle informa-

---

[5] Wisconsin S.C., State v. Loomis, 881, Wis. 2016; v. anche Indiana S.C., Malenchick v. State, 928, Ind. 2010.

[6] Circa gli algoritmi predittivi, le *guidelines* e i *warning* enunciati nella sentenza Loomis sono commentati in *Harvard Law Review*, 2017, Vol. 130: 1530-1537, e da E. Istrani, *Algorithmic Due Process: Mistaken Accountability and Attribution in State v. Loomis*, in *Harvard JOLT Digest*, 31 agosto 2017.

zioni utili per la valutazione del rischio nel mondo reale, e agli eventuali pregiudizi discriminatori, sono riusciti a frenare l'impetuosa avanzata delle tecniche informatiche di tipo predittivo nel sistema statunitense della giustizia penale[7].

Si è forse agli inizi di uno sconvolgente mutamento dello scenario classico della giurisdizione penale, in un profondo e inquieto rimescolamento delle coordinate tipiche dei due paradigmi, indiziario e galileiano, che non si atteggiano più come concettualmente distinti e autonomi? A fronte della complessità tecnica, della fallibilità e della fatica delle tradizionali operazioni giudiziali ricostruttive del fatto, la postmodernità sta mettendo in crisi l'equità, l'efficacia e le garanzie del modello del razionalismo critico, oppure resta ben salda e vitale l'arte del giudicare, seppure "*reasonig under uncertainty*" e "*by probabilities*"? Quali saranno le nuove frontiere delle strategie di *crime control* per la giustizia penale: dalla giustizia "giusta" alla utopica giustizia "esatta"[8]?

4. Giustizia predittiva e standard "*debole*" dell'IA

Le decisioni delle Corti statunitensi hanno suscitato – com'era largamente prevedibile – serie e fondate critiche da parte della comunità dei giuristi con riguardo al rischio di distorsioni cognitive dello stesso algoritmo (*Bias Automation*), per l'opacità del database, l'indeterminatezza del codice sorgente, l'automatica implementazione del *software*, l'accreditamento di pratiche discriminatorie.

Di qui l'intervento della comunità internazionale, diretto ad assicurare che l'utile arricchimento delle fonti informative del giudice e le predizioni del modello statistico-matematico mediante l'utilizzo di tecnologie computazionali si coniughino con il nucleo epistemologico tradizionale delle garanzie del giusto processo e rispondano comunque a criteri di controllo e specifica responsabilità dell'uomo.

Secondo le linee guida tracciate dalla *Carta etica sull'uso dell'intelligenza artificiale nei sistemi giudiziari e nel loro ambiente*, adottata il 3 dicembre 2018 dalla Commissione europea per l'efficienza dei sistemi di giustizia (CEPEJ), la coerenza logica del calcolo algoritmico va verificata in un processo d'integrazione fra le misurazioni quantitative, ricche e imponenti, da esso offerte con il percorso cognitivo e decisorio del giudice, nel rispetto dei metavalori dell'ordinamento.

---

[7] Negli USA, fino al 2020, non si registra l'utilizzo di *Risk Assessment Tools* in soli due Stati: Massachussets e New Hampshire.

[8] V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*,, 2020, 547 ss.

Insomma, sembra avere titolo ad accedere al processo penale soltanto lo standard "*debole*" (collaborativo) della intelligenza artificiale, che, nel dialogo e nella complementarità uomo-macchina[9], consenta comunque all'uomo di mantenere il controllo della macchina. Come, d'altra parte, già avvertiva la S.C. del Wisconsin nella sentenza *Loomis* (il software COMPAS "*… should be always constitute merely one tool available to a Court, that need to be confirmed by additional sound information…*"), le linee guida della Carta etica rimarcano il criterio della non esclusività del dato algoritmico per la decisione, che dev'essere viceversa riscontrato – corroborato – da ulteriori e diversi elementi di prova. Nello stesso senso è anche la prescrizione dettata dall'art. 8 del d.lgs. 18/05/2018, n. 51, Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27/04/2016, relativa 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 o esecuzione di sanzioni penali[10].

Come pure meritano rilievo gli ulteriori criteri di validazione indicati dalla Carta etica, in punto di garanzie dei diritti fondamentali della persona, di non discriminazione, di trasparenza, imparzialità, equità e comprensibilità dei metodi di elaborazione dei dati informatici, di controllabilità dei percorsi di calcolo, di qualità e attendibilità scientifica del risultato.

Dunque: *fitness*, ma anche *discovery*, *corroboration*, *accountability*, in un quadro di autonomia e responsabilità del decisore[11].

5. *Digital Evidence* e processo penale

Occorre ora porsi una serie di domande. Come organizzare correttamente l'accesso, nell'ambiente del processo penale, di questo tipo di *electronic evidence*, un peculiare sottoinsieme della prova scientifica e tecnologica, al fine di

---

[9] L. Floridi, *Robots, Jobs, Taxis and Responsabilities*, in *Philos. Technolog.*, 2017, 2: «*The best chess player is neither a human nor a computer, but a human using a computer*».

[10] Art. 8: "1. Sono vietate le decisioni basate unicamente su un trattamento automizzato, compresa la profilazione, che producano effetti negativi per l'interessato, salvo che siano autorizzati dal diritto dell'Unione europea o da specifiche disposizioni di legge. 2. Le disposizioni di legge devono prevedere garanzie adeguate per i diritti e le libertà dell'interessato. In ogni caso è garantito il diritto di ottenere l'intervento umano da parte del titolare del trattamento".

[11] Cons. V. Manes, op. loc. cit.; P. Severino, *Intelligenza artificiale e diritto penale*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, 2020, 531 ss.; R. Bichi, *Intelligenza digitale, giurmetria, giustizia predittiva e algoritmo decisorio.* Machina sapiens *e il controllo della giurisdizione*, *ivi*, 423 ss.

implementare la qualità delle *performance* cognitive e decisionali del giudicante? Come assicurare che sulla prova così acquisita trovi spazio l'esercizio del diritto di difesa, attraverso il confronto dialettico, la confutazione, la prova contraria, il dubbio? Come garantire il contraddittorio "*per*" e "*sulla*" prova, in funzione della validazione scientifica del risultato e contro la deriva tecnocratica della giurisdizione? Sono noti i criteri enunciati dalla Corte Suprema statunitense nella nota sentenza *Daubert*[12], in base ai quali il giudice deve vagliare l'effettiva affidabilità di una teoria o un metodo e di una *expert witness's scientific testimony*, ai fini della loro ammissibilità come prova scientifica nel processo: la controllabilità mediante esperimenti; la falsificabilità mediante test di smentita con esito negativo; la *peer review* della comunità scientifica di riferimento; la conoscenza della percentuale di errore dei risultati; infine, il criterio subordinato e ausiliario della generale accettazione da parte della comunità degli esperti. La Corte di Cassazione italiana[13], nel condividere sostanzialmente il *Daubert standard*, ne ha arricchito la portata, con riguardo alla fase della valutazione giudiziale della prova scientifica, aggiungendo i criteri dell'indipendenza e dell'affidabilità dell'esperto, l'ampiezza e il rigore del dibattito critico che hanno accompagnato la ricerca, le finalità e gli studi che la sorreggono, l'attitudine esplicativa dell'elaborazione teorica.

6. Il contraddittorio "*per*" la prova e l'art. 189 c.p.p.

Ma risulta davvero efficace rinviare la verifica della coerenza logica di questa speciale categoria di prova tecnologica al contraddittorio "*sulla*" prova, quando essa sia stata già ammessa e acquisita e le parti siano ormai posizionate dentro il dibattimento? Oppure sarebbe più utile costruire, nell'organizzazione del processo, un filtro di accesso, preventivo e a maglie strette, al fine di escludere – all'esito di un contraddittorio "*per*" la prova – addirittura che entrino nel patrimonio probatorio informazioni non sorrette da legittima validazione scientifica? La scienza e la tecnologia irrompono nel crogiuolo dell'esperienza giuridica. Ciò comporta che il funzionamento delle Corti, nelle questioni in cui sono coinvolte dimensioni tecniche e scientifiche, soprattutto se nuove per l'interprete, debba essere più flessibile, quanto al controllo delle parti sulle modalità di assunzione della prova, alla *discovery* e al contraddittorio, nel momento e in funzione sia

[12] Daubert v. Merrel Dow Pharmaceuticals, Inc., 509 US 579 (1993).

[13] Cass., Sez. IV, 17 settembre 2010, n. 43786, Cozzini, sull'attendibilità di una teoria relativa all'eziologia del cancro dovuta ad esposizione all'amianto. Cons. anche Cass, Sez. Un., 11 settembre 2002, n. 30328, Franzese, sulle leggi scientifiche di copertura del nesso causale tra la condotta omissiva del medico e l'evento lesivo in danno del paziente.

dell'ammissione che della valutazione della prova, e, dall'altro, più rigoroso quanto alla verifica di attendibilità del risultato probatorio. Merita di essere segnalato, in proposito, un passo della Relazione al Progetto preliminare del nuovo codice di procedura penale del 1989 (p. 60), riguardante la portata dell'art. 189 c.p.p.: «*È sembrato che una norma così articolata possa evitare eccessive restrizioni ai fini dell'accertamento della verità, tenuto conto del continuo sviluppo tecnologico che estende le frontiere dell'investigazione, senza mettere in pericolo le garanzie difensive*». Norma cardine, questa, nell'*intentio legis*, diretta ad assicurare, con l'apporto della scienza nella ricerca della verità, l'opportuna flessibilità del sistema processuale in materia di prova scientifica o tecnologica nuova. L'apprezzamento di rilevanza, non superfluità e concreta idoneità (*fitness*) della prova "*ad assicurare l'accertamento dei fatti*" – senza che ne resti pregiudicata "*la libertà morale delle persone*" (quanto al divieto di perizia criminologica *ex* art. 220, comma 2 c.p.p.) – è rimesso al vaglio critico del giudice. Allo scopo di garantire l'anticipata conoscenza delle parti circa le metodologie che saranno applicate nell'accertamento, il Giudice, dopo avere sentito le parti sulle modalità di assunzione della prova, provvede all'ammissione con ordinanza, fissando le regole per la corretta applicazione dei metodi e delle procedure tecniche di acquisizione della stessa. Come si vede, un filtro, questo dell'art. 189, a maglie ben più strette rispetto a quello previsto dall'art. 190, comma 1, che, ai fini dell'ammissione della prova in genere, si limita a selezionare negativamente solo «*le prove vietate dalla legge e quelle che manifestamente sono superflue o irrilevanti*»: un filtro, inoltre, che è assistito da un significativo rafforzamento del contraddittorio anticipato, "*per*" la prova, ancor prima che "*sulla*" prova.

7. Qualche conclusione provvisoria

La diga finora eretta dalla comunità internazionale dei giuristi con il rigoroso disciplinamento, etico e giuridico, del fenomeno sta – per ora – reggendo l'urto impetuoso e intrigante, nel contesto del processo e di quello penale in particolare, delle pervasive tecnologie dell'intelligenza artificiale. Non sembra dunque che sia in corso uno sconvolgente e non auspicabile mutamento di paradigma della struttura e della funzione della giurisdizione penale (col rischio di incorrere nell'opposta fallacie dell'automazione – *automation bias* –) e che, a fronte della complessità tecnica, dei tempi e dei costi delle faticose operazioni giudiziali ricostruttive del fatto, la postmodernità stia mettendo in crisi l'equità, l'efficacia e le garanzie del modello proprio del razionalismo critico, insieme con la tradizionale arte del giudicare, *reasonig under uncertainty* e *by probabilities*. Il diritto penale del fatto è incentrato sulla persona umana e il metodo dialettico

dell'accertamento **è** affidato al giudizio dell'uomo: verosimilmente fallibile e però controllabile secondo legge e ragione. Sicché resta tuttora precluso il decidere senza giudicare.

Ma gli esiti della nuova sfida lanciata dal progresso della scienza non sono affatto scontati. Al bivio tra tecnologia e tecnocrazia, dinanzi all'irruzione del modello "*forte*" dell'IA, ancora una volta la sfida si sposta, a ben vedere, sul terreno della concreta efficacia e qualità del sistema processuale.

La moderna ricerca socio-giuridica, anche alla luce delle prassi applicative già in corso in alcuni Paesi, auspica che l'approccio della giurisdizione al fenomeno dell'IA si basi su una metodologia estremamente pragmatica. Non vi è dubbio che il livello di efficacia, qualità e prevedibilità della giurisdizione penale sarebbe più alto ed apprezzabile se essa venisse esercitata nell'ambito di una procedura articolata in una dinamica interazione fra i saperi e le operazioni logiche tradizionalmente affidate al giudice e alle parti, da un lato, e le evidenze della prova informatica o di quella digitale o del calcolo di un algoritmo, dall'altro.

È infatti cresciuta nella società la legittima pretesa che il giudice, nell'esercizio dell'arte del giudicare e nella pratica giudiziaria, sia un buon ragionatore e un decisore di qualità. Sicché la professionalità, l'etica e l'implementazione del grado di *expertise* accumulata dal giudice (e dai difensori) nell'utilizzo delle tecniche inferenziali del ragionamento e nella verifica degli schemi statistico-probabilistici, acquisiti con l'ausilio della tecnologia digitale, di *software* informatici e algoritmi predittivi o con l'apporto della robotica e della logica dell'IA, potrebbero certamente contribuire a restituire al funzionamento della giustizia penale una più adeguata immagine di efficacia e qualità.

Francesco Caprioli

Intercettazioni e tutela della *privacy* nella cornice costituzionale

SOMMARIO: 1. Intercettazioni e segretezza delle comunicazioni. – 2. Intercettazioni e intimità domiciliare. – 3. Le videointercettazioni domestiche nel quadro costituzionale. – 4. Segretezza, segreto, riservatezza, *privacy*. – 5. Il diritto all'inaccessibilità della sfera privata. – 6. L'interesse al segreto sui dati esteriori della comunicazione. – 7. La diffusione del documento sonoro o audiovisivo. – 8. Intercettazioni e riservatezza. – 9. Intercettazioni e trattamento dei dati personali. – 10. Processo penale e riservatezza: lesioni inevitabili e lesioni gratuite.

1. Intercettazioni e segretezza delle comunicazioni

L'analisi dei rapporti tra le attività di intercettazione e il diritto alla *privacy* non può che muovere dall'art. 15 della Costituzione. Chi intercetta percepisce comunicazioni indirizzate ad altri, accedendo a un canale comunicativo che, per volontà del mittente, dovrebbe essergli precluso. Per ciò solo – ma sul punto occorrerà tornare – si tratta di un'attività lesiva del diritto alla libertà e alla segretezza delle comunicazioni.

L'atto investigativo indiscreto deve pertanto soddisfare le condizioni fissate dal precetto costituzionale. In primo luogo, occorre un provvedimento motivato dell'autorità giudiziaria: preso alla lettera, l'art. 15 Cost. non contiene un'autentica riserva di giurisdizione, lasciando aperto il problema della conformità al dettato costituzionale di un assetto normativo che attribuisse al pubblico ministero un autonomo potere di disporre le intercettazioni. Occorre notare, per contro, che non sono contemplate limitazioni provvisorie della segretezza ad opera degli organi di polizia, a differenza di quanto stabilito negli artt. 13 e 14 Cost. per le limitazioni della libertà personale e dell'intimità domiciliare: quasi certamente si è trattato di una dimenticanza dei Costituenti, ma c'è chi spiega la scelta di maggiore cautela in ragione della particolare natura di questi attentati alla sfera personale dell'individuo, che coinvolgono necessariamente, in un'indagine penale, anche soggetti estranei al reato per cui si procede. In secondo luogo, le limitazioni sono consentite con le "garanzie stabilite dalla legge": clausola che deve intendersi come riferita anche alla necessaria individuazione "dei casi e dei modi" di aggressione alla sfera individuale, sulla falsariga di quanto espres-

samente previsto per la libertà personale e l'intimità del domicilio. Indicazioni preziose provengono, al riguardo, dalla giurisprudenza della Corte Europea dei diritti dell'uomo in tema di intrusioni legalmente previste nella vita privata delle persone (art. 8 Conv. Eur.): le fattispecie limitative devono caratterizzarsi sia per la loro chiarezza e accessibilità al cittadino comune, sia per la loro precisione, ossia per la dettagliata individuazione delle circostanze e delle condizioni in presenza delle quali l'autorità statale può violare la vita privata. L'esigenza di fondo è che l'ingerenza sia ragionevolmente preventivabile dall'interessato, in modo che quest'ultimo sia in grado di regolare la sua condotta in proposito.

Su quest'ultimo punto si è registrata qualche interessante novità nel recente dibattito dottrinale. La disciplina italiana delle intercettazioni soffre da sempre di un evidente *deficit* di tipicità. Per cominciare, il codice disciplina le attività di intercettazione senza fornire alcuna definizione del concetto, che viene dato interamente per scontato dal legislatore. Sono state la dottrina e la Corte di Cassazione (in particolare, la sentenza Torcasio del 2003) a ritagliare i contorni del *genus*, nei termini che ben conosciamo: la comunicazione deve avere carattere riservato (nel senso che deve svolgersi con *modalità* che rivelino oggettivamente la volontà del mittente di riservare la percezione delle sue parole a una cerchia delimitata di soggetti, non comprensiva dell'autore dell'intercettazione); l'ascolto non deve essere meramente "fisiologico" (cioè deve essere effettuato mediante strumenti tecnici di percezione); il dispositivo deve consentire la percezione del colloquio e non soltanto la registrazione di quanto viene fisiologicamente percepito. Ma qualche importante aspetto rimane in ombra: non è affatto chiaro, ad esempio, se le operazioni di ascolto debbano essere effettuate all'insaputa del solo mittente della comunicazione riservata o anche del suo destinatario (o dei suoi destinatari). Va inoltre osservato che nessun criterio legale è dettato per l'individuazione delle utenze telefoniche e/o degli ambienti da monitorare: purché "indispensabile per la prosecuzione dell'indagine" – criterio assai meno selettivo di quanto possa apparire –, l'ascolto clandestino può estendersi a macchia d'olio a discrezione degli inquirenti.

Questa definizione alquanto approssimativa dei casi e dei modi di aggressione al diritto costituzionale è sempre stata tollerata con una certa disinvoltura dagli interpreti. Il dibattito si è riacceso quando i pubblici ministeri hanno cominciato a utilizzare come strumento di intercettazione i captatori informatici.

Non c'è dubbio che nel modello normativo elaborato dalla sentenza Torcasio potesse già farsi rientrare – prima della legge Orlando e poi della legge Bonafede – anche l'ascolto clandestino effettuato per il tramite del dispositivo informatico contagiato: sarebbe stato ingeneroso affermare che quelle micidiali pratiche investigative avvenissero nel silenzio della legge processuale. Si era tuttavia aperta una disputa. L'opinione di molti era che per rispettare l'art. 15 Cost.

(e le riferite indicazioni provenienti dalla Corte Europea dei diritti dell'uomo) fosse indispensabile un immediato intervento normativo. Altri lo negavano recisamente, osservando che se fosse necessaria una specifica previsione di legge per ogni tipologia di strumento captativo utilizzabile (ieri le microspie, oggi i captatori informatici, domani chissà), il legislatore si troverebbe costretto a inseguire affannosamente i progressi della tecnica, con risultati inevitabilmente parziali e tardivi: molto meglio, si diceva, tracciare una cornice "aperta" di garanzie fondamentali nella quale si possano inscrivere i dispositivi di ascolto già esistenti, quelli nuovi e quelli futuri. Era un'opinione ragionevole, che si esponeva tuttavia a una banale obiezione. Al variare delle tecniche intrusive variano le garanzie: una tecnica di intercettazione come quella basata sul captatore informatico comporta la necessaria previsione di garanzie individuali *ad hoc*, che valgono solo con riferimento a quello specifico strumento captativo. Si pensi, per fare qualche esempio, alla necessità di evitare che il *malware* determini un abbassamento del livello di sicurezza del dispositivo su cui viene usato, alla necessità di garantirne la disinstallazione a intercettazione conclusa, ai problemi legati alla natura non "stanziale" del dispositivo ospite e alla conseguente necessità di regolare i tempi di accensione e spegnimento da remoto ecc. Merita dunque apprezzamento, almeno sotto questo profilo, l'aggiornamento legislativo della disciplina dell'intercettazione cui hanno provveduto le recenti riforme. Sul piano generale, s'intende che certi dettagliati protocolli operativi non sono materia per un codice di procedura penale: ma nel 2009, quando è stata finalmente regolata la materia delle perizie che incidono sul diritto alla libertà personale, il legislatore si è occupato del prelievo di mucosa del cavo orale e di altre simili pratiche tecnico-scientifiche senza destare particolare scandalo.

2. Intercettazioni e intimità domiciliare

Le attività di intercettazione comportano poi, in taluni casi, anche una diretta e immediata lesione dell'intimità domiciliare, cioè sono compiute in violazione dell'art. 14 Cost.

Sul punto conviene evitare fraintendimenti. L'art. 266 comma 2 c.p.p. pretende, notoriamente, condizioni particolarmente restrittive (il *fumus perdurantis criminis*) quando a essere intercettata sia una comunicazione tra presenti che si svolge nel domicilio o in altri luoghi di privata dimora. Si potrebbe pensare che in questo modo il legislatore abbia voluto offrire una tutela rafforzata della segretezza delle comunicazioni domiciliari, sul presupposto di una loro natura, per così dire, iper-riservata (è ovvio che chi parla nel proprio domicilio non intende essere ascoltato da terzi estranei). Ma non è così: se la comunicazione si svolge

con modalità riservate, non v'è ragione di proteggerla più o meno intensamente a seconda del luogo in cui si svolge. Quelle maggiori cautele sono state previste dal legislatore perché un'attività di intercettazione di colloqui domiciliari *comporta necessariamente un attentato all'intimità domiciliare* (al quale, a volte, non si affianca alcuna lesione della segretezza delle comunicazioni). Il legislatore è consapevole del fatto che se l'inquirente introduce una microspia in casa d'altri (oggi, un captatore informatico in uno *smartphone* che transita all'interno di un domicilio), quel dispositivo non può selezionare le comunicazioni dagli altri suoni: tutto viene percepito e registrato. A verificarsi, dunque, se la casa non è disabitata, sono indebite intrusioni nell'intimità domiciliare che spesso non hanno nulla a che fare con una intercettazione di comunicazioni, e nulla hanno a che vedere con l'art. 15 Cost. La microspia permette all'inquirente un ingresso sensoriale nel domicilio altrui che è a tutti gli effetti una violazione dell'art. 14 Cost. Inoltre, lo strumento di ripresa sonora potrebbe percepire suoni che documentano inequivocabilmente un'attività domestica non comunicativa che l'interessato preferirebbe sottrarre alla conoscenza dei terzi: ad esempio, che si diletta a guardare certi film, che recita una preghiera, che inveisce ad alta voce contro un politico che sta parlando alla tv (sempre che le preghiere e le invettive solitarie non siano comunicazioni: sembrerebbe da escludere, ma la questione rimane aperta). L'art. 266 comma 2 c.p.p. va inteso in questa chiave: cautele ulteriori, presupposti più restrittivi perché occorreva soddisfare anche la riserva di legge contenuta nell'art. 14 Cost. (per le "vecchie" intercettazioni domiciliari effettuate per il tramite di una microspia anziché di un captatore informatico, c'è anche il problema della violazione "fisica" del domicilio che talvolta è necessaria per installare il dispositivo di ascolto).

Questo ancora non significa che quei suoni e quei rumori sintomatici di comportamenti non comunicativi siano utilizzabili come prova: il codice è sufficientemente esplicito nello stabilire che l'unico risultato utilizzabile di un'intercettazione sono le "comunicazioni" intercettate. Ma ciò non toglie che le attività di intercettazione che si svolgono in un domicilio – più esattamente, le lesioni dell'intimità domiciliare che si realizzano per il tramite di un'attività investigativa volta all'intercettazione di colloqui domestici – siano previste nei casi e nei modi dal legislatore in ossequio all'art. 14 Cost.

3. Le videointercettazioni domestiche nel quadro costituzionale

Queste premesse sono utili per inquadrare correttamente una delle più delicate ipotesi di attrito tra intercettazione e *privacy*: la video-intercettazione, e, in particolare, la video-intercettazione domiciliare.

Molto spesso si ragiona in questi termini (lo hanno fatto anche la Corte di Cassazione e la Corte Costituzionale). Le video-intercettazioni sono consentite, perché la legge non stabilisce affatto che gli strumenti di intercettazione debbano essere necessariamente strumenti di ripresa sonora e non anche strumenti di ripresa visiva (come fare, del resto, con i dialoghi tra sordomuti?). E le video-intercettazioni, come tutte le intercettazioni, sono consentite anche nel domicilio, se effettuate nel rispetto dei parametri di cui all'art. 266 comma 2 c.p.p. Fin qui nulla da eccepire: anche se tornano ad affacciarsi i dubbi di scarso rispetto degli artt. 14 e 15 Cost. nella parte in cui richiedono l'individuazione dettagliata dei casi e dei modi dell'intercettazione. Ma che ne è delle riprese audio-video di comportamenti non comunicativi? Si dice: l'attività captativa, in quella sua parte, non è più un'intercettazione, ma un'attività di ricerca della prova *non disciplinata dalla legge* che incide sul diritto alla intimità domiciliare. *Ergo*, quelle riprese non sono utilizzabili come prova.

È una ricostruzione che convince poco. Davvero si può pensare che l'inutilizzabilità della prova basti a rendere innocuo il gravissimo attentato all'intimità domiciliare che si sarebbe nel frattempo consumato in violazione dell'art. 14 Cost.? La Corte Europea ha già avuto modo di chiarirlo: la lesione dei diritti di *privacy* – con ciò che ne segue anche in termini di attribuzione di poteri di reclamo al loro titolare (sia esso l'indagato o un soggetto terzo) – si determina a prescindere dall'uso processuale dei materiali che ne costituiscono il frutto. Immaginiamo, del resto, che nel corso di un'operazione di intercettazione una persona venga ripresa all'interno di un domicilio in comportamenti non comunicativi di natura privata. Il domicilio è legittimamente monitorato perché un altro degli occupanti di quella casa è indagato per gravi reati di cui si teme lo svolgimento attuale *ex* art. 266 comma 2 c.p.p. Venuto a conoscenza di quella grave lesione della sua intimità domiciliare, il soggetto ripreso, che nulla sa di quei fatti e di quell'indagine, protesterebbe vigorosamente: era consentita quella sorveglianza elettronica? Assolutamente no, gli dovremmo rispondere, perché i tuoi comportamenti non erano comunicativi, e la legge non prevede lesioni di questo tipo dell'intimità domiciliare che non si accompagnino alla lesione della segretezza delle comunicazioni. La violazione è avvenuta senza alcuna base legale in grado di soddisfare la riserva di legge di cui all'art. 14 Cost. Però niente paura: quelle prove non sono utilizzabili. Magra consolazione: l'interessato risponderebbe, ovviamente, che non gli importa nulla se quelle riprese audiovisive avranno o meno valore di prova in un processo che non lo riguarda e di cui neppure conosce l'esistenza.

Molto meglio ragionare nell'altro modo. Quella violazione dell'art. 14 Cost. era prevista e regolata dalla legge: le intercettazioni (e le video-intercettazioni) domiciliari sono consentite sulla base di presupposti più rigorosi proprio perché quell'attività investigativa, pur diretta a captare comunicazioni, comporta anche e

inevitabilmente un sacrificio dell'intimità domiciliare. Al malcapitato coinquilino della casa videosorvegliata potremmo dire: sì, gli inquirenti potevano fare quello che hanno fatto, la violazione del tuo diritto all'intimità domiciliare poggiava su una specifica base legale, la legge si fa carico del sacrificio che ti è stato imposto.

Un problema analogo si era posto con le intercettazioni effettuate mediante il captatore informatico, quando ancora la materia non era stata regolata dalla legge e non era così chiaro se lo strumento di ripresa sonora annidato nel dispositivo mobile potesse venire attivato e disattivato a intermittenza da remoto. Anche qui l'attentato alla *privacy* avveniva con l'ausilio di uno strumento tecnico-scientifico le cui potenzialità intrusive sfuggivano a un pieno controllo dell'operatore. Nel caso delle riprese audio-video di comportamenti domiciliari, il problema, come detto, è che lo strumento di ripresa non è in grado di distinguere il tipo di condotta che viene documentata. Nel caso del captatore informatico inoculato in uno *smartphone*, il problema – ulteriore – era la natura non stanziale del dispositivo ospitante, che, spostandosi in luoghi pubblici e privati, era inevitabilmente destinato a captare (se non controllabile da remoto) comunicazioni domiciliari ed extradomiciliari. Si profilava nuovamente il rischio che alle legittime violazioni della segretezza delle comunicazioni si affiancassero illegittime violazioni dell'intimità domiciliare, dovute, ancora una volta, all'attitudine "onnivora" dello strumento di intercettazione. Le Sezioni unite Scurato del 2016 avrebbero dunque potuto ragionare come la giurisprudenza in materia di videoriprese domiciliari: inutilizzabili le conversazioni domiciliari (se l'intercettazione non era stata autorizzata *ex* art. 266 comma 2 c.p.p.), utilizzabili quelle registrate dallo *smartphone* fuori del domicilio. E invece la Corte di Cassazione – molto opportunamente – aveva ragionato in tutt'altro modo: la sanzione dell'inutilizzabilità non si adatta «ad ipotesi di adozione di provvedimenti […] *non preventivamente controllabili quanto alla loro conformità alla legge*», anche perché c'è «il concreto rischio della possibile divulgazione, ben prima della declaratoria di inutilizzabilità, dei contenuti di intercettazioni destinate ad essere successivamente dichiarate inutilizzabili». Dunque, si disse, niente intercettazioni realizzate con i *Trojan horses* (salvo che nei procedimenti per reati di criminalità organizzata), perché ci sarebbe il rischio di violare l'intimità domiciliare e la segretezza delle comunicazioni anche in casi in cui la legge non lo consente.

4. Segretezza, segreto, riservatezza, *privacy*

Fin qui gli attentati alla segretezza delle comunicazioni e all'intimità domiciliare. Le intercettazioni comportano però, naturalmente, anche gigantesche violazioni della riservatezza delle persone i cui colloqui vengono intercettati e delle

persone di cui si parla in quei colloqui. In proposito, conviene in primo luogo operare qualche distinzione concettuale: diritto alla segretezza delle comunicazioni, diritto al segreto sull'oggetto della comunicazione, diritto alla riservatezza, diritto alla *privacy*.

Chi comunica con altre persone (per iscritto o a voce) può desiderare in primo luogo che le sue parole non siano lette o ascoltate da persone diverse dal destinatario della comunicazione. Il diritto alla segretezza della comunicazione sta esattamente in questa pretesa di salvaguardare l'intimità del rapporto comunicativo: è il diritto del mittente di impedire che soggetti diversi dal destinatario percepiscano – nel caso della comunicazione orale, ascoltino – il messaggio trasmesso. L'autore di una comunicazione riservata offre all'interlocutore – gli "riserva", appunto – un'immagine esclusiva della propria persona la cui intimità va tenuta al riparo dallo sguardo indiscreto dell'ascoltatore clandestino.

L'espressione "comunicazione riservata" può ingenerare qualche equivoco: conviene ribadire che si sta parlando del *modo* con cui si comunica, non del *contenuto* della comunicazione. I radioamatori che comunicano via radio su frequenze accessibili a chiunque o gli abitanti della casa del Grande Fratello non possono ovviamente pretendere che l'intimità delle loro comunicazioni sia tutelata. Ma se l'atto comunicativo è riservato, la sua segretezza deve essere tutelata a prescindere dal contenuto della comunicazione. Si pensi, del resto, alla tutela penale delle comunicazioni riservate: chi prende cognizione di una lettera chiusa indirizzata ad altri o intercetta una comunicazione telefonica è punito quale che sia il contenuto della missiva o della conversazione telefonica. Come scriveva Vincenzo Manzini tanti anni fa, non importa nulla che quella comunicazione contenga la più intima delle confidenze o la descrizione di una pianta officinale. Né si tratta di una semplice anticipazione della tutela penale: non si protegge il contenitore (la comunicazione riservata) per proteggere un eventuale contenuto (la notizia segreta eventualmente comunicata). Oggetto di tutela è la comunicazione riservata in quanto tale, l'intimità dell'individuo nell'atto – personalissimo – di comunicare riservatamente. La dottrina tedesca definisce *dialogisches Prinzip* qualcosa di molto simile: il diritto di decidere spontaneamente *a chi destinare le proprie parole*, se al solo partner, a un certo gruppo di persone o al pubblico.

Il mittente di una comunicazione orale può poi naturalmente desiderare che nessuna persona all'infuori del destinatario (e di altri soggetti eventualmente legittimati a conoscere) *apprenda i fatti* che costituiscono l'oggetto della comunicazione stessa. Si tratta di quello che può essere definito interesse *al segreto* sull'oggetto della comunicazione: il quale, in realtà, non è che l'eventuale ulteriore interesse di carattere personale, economico, professionale ecc. che di volta in volta giustifica – connotandolo in chiave assiologica – il desiderio di sottrarre il contenuto dell'atto comunicativo alla conoscenza dei terzi. L'ordinamento può

proteggere in vario modo questo interesse: si pensi alla disciplina del segreto professionale, del segreto industriale, del segreto di Stato ecc. Nulla a che vedere con la segretezza della comunicazione: chi costringe il destinatario di una comunicazione riservata a testimoniare sul contenuto del colloquio non sta certamente violando la segretezza (non occorre la previsione dei casi e dei modi per indurre un testimone a violare un vincolo confidenziale); *idem* se il depositario della confidenza rivela di sua iniziativa il contenuto del colloquio. Nessuno, cioè, ha mai pensato che basti immettere una notizia in un circuito comunicativo riservato (nel senso delle *modalità* di trasmissione del pensiero) perché quella notizia si ammanti della "segretezza" cui allude l'art. 15 Cost., cioè non possa essere rivelata dal suo destinatario o appresa da terzi se non nel rispetto delle condizioni fissate dalla norma costituzionale.

Quando oggetto della comunicazione riservata sono fatti che attengono alla vita privata del mittente o di altre persone, il diritto al segreto viene a coincidere con il diritto alla riservatezza, da intendersi come diritto al controllo sulla circolazione e sull'uso delle notizie che riguardano la propria sfera personale. La lesione della riservatezza non è dunque che *una conseguenza indiretta ed eventuale* della lesione della segretezza, cioè della profanazione dell'intimità del rapporto comunicativo che veicola la notizia attinente alla vita privata. La lesione della segretezza di un rapporto comunicativo non comporta necessariamente l'apprensione di notizie segrete o riservate (ossia di notizie, anche attinenti alla vita privata, che il mittente abbia un interesse giuridicamente rilevante a mantenere confinate in una sfera di conoscenza limitata), così come, ovviamente, le notizie segrete o riservate possono essere apprese anche senza violare la segretezza di una comunicazione. Le Sezioni Unite D'Amuri del 2000 lo avevano opportunamente ribadito (riprendendo una classificazione proposta da chi scrive quasi dieci anni prima): esistono condotte lesive della segretezza che non sono lesive della riservatezza e viceversa, ed esistono condotte lesive a un tempo di entrambi i diritti costituzionali.

5. Il diritto all'inaccessibilità della sfera privata

Lo stesso *è a dirsi* per il diritto alla intimità domiciliare.

L'art. 14 Cost. impedisce ai terzi, in primo luogo, di introdursi e trattenersi fisicamente in casa d'altri: ma è ormai pacifico che il precetto costituzionale precluda anche gli ingressi meramente sensoriali nell'altrui domicilio, realizzati attraverso apparecchi di ripresa visiva o sonora. Il divieto di intrusioni (fisiche o sensoriali) nella sfera domiciliare mira ad assicurare all'individuo uno spazio inviolabile di libera estrinsecazione della propria personalità, una "zona protetta"

dall'altrui invadenza in cui egli possa sottrarsi ad ogni condizionamento esterno che coinvolga la sua persona. Anche l'art. 14 Cost. tutela dunque in via meramente eventuale e indiretta il diritto alla riservatezza. È una mera eventualità che l'atto intrusivo conduca anche all'apprensione di notizie segrete attinenti alla vita privata (una videocamera che riprende una persona mentre dorme o mentre prende un caffè in casa sua non sta certamente catturando notizie private che quella persona abbia interesse a mantenere segrete, ma sta altrettanto certamente violando la sua intimità domiciliare).

L'analogia con il diritto alla segretezza delle comunicazioni è molto evidente. Nello spazio fisico delimitato dalle mura domestiche e nello spazio ideale segnato dalla riservatezza del rapporto comunicativo, ogni privata manifestazione dell'individuo deve rimanere sottratta alla indebita percezione dei terzi. Come il domicilio, secondo una vecchia e celebre definizione, è la "proiezione spaziale" della persona, la comunicazione riservata – scriveva Franco Bricola – è la sua "proiezione spirituale". E come l'art. 14 Cost. impedisce a chiunque di guardare in casa d'altri (ad esempio, installando una telecamera), così l'art. 15 Cost. vieta a chiunque di ascoltare comunicazioni che non sono dirette a lui. Anche l'art. 15 intende assicurare all'individuo uno spazio privilegiato e inaccessibile di libera manifestazione della propria personalità: con la sola differenza, rispetto alla tutela dell'inviolabilità domiciliare, che si tratta dello spazio "ideale" segnato dalla esclusività e riservatezza del rapporto comunicativo anziché dello spazio fisico delimitato dalle mura domestiche.

In sintesi, nei confini dell'intimità domiciliare e delle comunicazioni riservate, ogni privata manifestazione dell'individuo deve rimanere sottratta alla indebita percezione dei terzi. Segretezza delle comunicazioni e inviolabilità del domicilio concorrono nell'assicurare all'individuo quello che può essere definito il diritto costituzionale *all'inaccessibilità (o intimità) della propria sfera privata*, da intendersi come diritto a coltivare la propria personalità in ambiti spirituali (la comunicazione riservata) e spaziali (il domicilio) sottratti all'ascolto e all'osservazione degli estranei. Quando si parla di *privacy* – o, in una prospettiva europea, di «rispetto della vita privata» – il riferimento deve intendersi indirizzato sia a questo primario diritto all'inaccessibilità (per così dire, sensoriale) della propria vita privata, sia al diritto alla riservatezza, ossia al diritto al controllo sulla circolazione e sull'uso delle notizie personali. Ma conviene ripeterlo ancora: l'interesse al segreto su quanto avviene all'interno del domicilio o viene comunicato riservatamente – vale a dire, l'interesse a impedire che i terzi non autorizzati *apprendano le notizie segrete* attinenti alla vita privata domiciliare o le notizie segrete oggetto della comunicazione riservata – riceve dagli artt. 14 e 15 Cost. una tutela meramente virtuale e riflessa.

6. L'interesse al segreto sui dati esteriori della comunicazione

Riassumendo, un'intercettazione lede certamente la segretezza della comunicazione: può ledere la riservatezza (del mittente o di altri) se consente di apprendere notizie riservate. Un'intercettazione di colloqui domiciliari *inter praesentes* lede certamente, se la casa non è disabitata, l'intimità del domicilio: può ledere la segretezza delle comunicazioni (se il microfono capta colloqui riservati) nonché la riservatezza (se vengono apprese notizie riservate).

Si sente dire spesso che nel momento dell'apprensione clandestina della notizia verrebbe violata la segretezza, nel momento della divulgazione della notizia verrebbe violata la riservatezza. Non è così: con l'ascolto clandestino che permetta all'intruso di venire a conoscenza di notizie riservate *è violata tanto la segretezza* (perché il terzo *ascolta* il colloquio) quanto la riservatezza (perché il terzo *apprende la notizia*): con la divulgazione si consumano *altre* lesioni della riservatezza, perché la notizia privata viene fatta *ulteriormente* circolare oltre la sfera di conoscenza delimitata dal suo titolare.

Una notizia riservata che si può apprendere tramite l'intercettazione è anche la notizia stessa che quella comunicazione si sia svolta. Chi comunica riservatamente può avere infatti un terzo interesse giuridicamente rilevante, oltre a quello di evitare ascolti indesiderati e circolazioni indesiderate delle notizie immesse nel canale comunicativo: può desiderare che nessuno all'infuori del destinatario sappia che quella comunicazione è avvenuta, quando e con quali modalità. In molti casi la notizia stessa che Tizio ha parlato a Caio può essere una notizia che Tizio ha interesse a mantenere all'interno di una sfera cognitiva soggettivamente limitata. Anche qui naturalmente occorrono caratteristiche oggettive della comunicazione che siano compatibili con un simile interesse: non è così, ad esempio, se Tizio e Caio conversano riservatamente (cioè in maniera che nessun altro ascolti) ma in un luogo pubblico.

Di questo interesse al segreto sui dati esteriori della comunicazione si è molto discusso in materia di tabulati telefonici. L'opinione prevalente (condivisa dalla giurisprudenza di legittimità e costituzionale) è che questo interesse sia direttamente protetto dall'art. 15 Cost., ma neppure questa è un'opinione convincente. Qui non c'è alcuna profanazione dell'intimità del rapporto comunicativo, non c'è alcun tentativo di infiltrazione sensoriale in quello spazio sacro di manifestazione della personalità dell'individuo che è la comunicazione riservata. L'inquirente acquisisce *notizie* che attengono alla sfera privata dell'individuo: siamo a pieno titolo nella dimensione concettuale del diritto alla riservatezza (e degli attentati a questo diritto).

7. La diffusione del documento sonoro o audiovisivo.

Queste premesse ricostruttive sono utili per inquadrare una fattispecie assai delicata, e cioè l'ipotesi in cui, dopo il primo ascolto della comunicazione riservata – sia esso legittimo oppure clandestino –, il destinatario della comunicazione, anziché limitarsi a riferirne a terzi il contenuto, diffonda senza l'autorizzazione del mittente la registrazione sonora del colloquio. In questi casi, a realizzarsi (o a perpetuarsi, se il primo ascolto è stato clandestino) è la lesione della segretezza, perché il terzo viene messo nelle condizioni di ascoltare la comunicazione riservata e non solo di apprenderne i contenuti eventualmente segreti.

Il tema assume rilevanza in due ambiti, cui non può essere qui dedicato che qualche breve cenno: la registrazione clandestinamente effettuata dall'interlocutore e la pubblicazione delle intercettazioni su cui sia caduto il segreto.

Sul primo versante, come è noto, la Corte di Cassazione ha escluso per lungo tempo che fossero ravvisabili lesioni della segretezza delle comunicazioni: la condotta di chi rivelava il contenuto di una comunicazione a lui rivolta e la condotta di chi faceva ascoltare a terzi la registrazione del colloquio venivano considerate due lesioni qualitativamente equivalenti della (sola) riservatezza. Se il destinatario di una comunicazione tradisce il vincolo confidenziale, poco importa, si diceva, che egli unisca a una ferrea memoria anche un supporto magnetico o digitale clandestinamente confezionato. Quanto si è detto in precedenza in ordine al fondamento del diritto alla segretezza delle comunicazioni smentiva questa semplicistica ricostruzione, che appariva, del resto, apertamente contraria al senso comune. La segretezza, in questi casi, è certamente violata, perché il terzo è messo nelle condizioni di percepire e non solo di sapere, diventa l'indebito fruitore dell'"immagine" comunicazionale che il mittente intendeva riservare al destinatario. Si è dunque fatta strada anche nella giurisprudenza di legittimità una diversa opinione. Il colloquiante infedele munito di registratore violerebbe il diritto tutelato dall'art. 15 Cost.: si tratterebbe però di una violazione non grave, attenuata, certamente non paragonabile a quella che si consuma nel caso dell'intercettazione. Non occorrerebbe dunque rispettare la riserva di legge e la riserva di giurisdizione: sarebbero sufficienti le "garanzie minime" rappresentate da un provvedimento del pubblico ministero motivato sulla base di esigenze investigative. È la logica dei valori di appartenenza all'insieme, la logica "*fuzzy*" che la nostra giurisprudenza, sempre più spesso, prende infaustamente a prestito dalla Corte Europea dei diritti dell'uomo (un altro esempio, in materia di videoriprese, sono i luoghi "semi-pubblici" della sentenza Prisco, che sono un po' domicilio e un po' no, e dunque possono essere monitorati sulla base di un semplice provvedimento del pubblico ministero). Derive pericolose, che generano incertezza e andrebbero evitate.

La seconda riflessione riguarda la pubblicazione delle intercettazioni sulle quali sia caduto il segreto. Chiunque istintivamente percepisce la profonda differenza che passa tra il riferire pubblicamente il contenuto di una certa telefonata intercettata non più coperta dal segreto – condotta del tutto legittima se quella notizia è rilevante nel processo – e il mettere direttamente a disposizione del pubblico la registrazione del colloquio, come ormai spesso accade nelle trasmissioni televisive di cronaca giudiziaria o sui siti web delle testate giornalistiche (spesso, tra l'altro, per lungo tempo: sul punto è dovuto intervenire il Garante della privacy) e senza il filtro di una pur minima semiosi umana (come la riproduzione integrale del testo con l'uso del virgolettato, o la rappresentazione "teatrale" del colloquio captato). Con la diffusione pura e semplice della registrazione il mittente viene "messo a nudo", viene mostrato nell'atto di comunicare: ai terzi non viene semplicemente trasmessa la conoscenza delle notizie (delle opinioni, delle sensazioni ecc.) veicolate dall'atto comunicativo. Sono tollerabili queste gravi ulteriori lesioni della segretezza? La legittima acquisizione al processo di quel documento sonoro azzera, accanto alle pretese di riservatezza, anche le pretese di segretezza di chi sia stato intercettato? Forse sì: garantire il controllo democratico su come viene amministrata la giustizia penale è un'esigenza che stenta a lasciarsi ingabbiare; il pubblico dei processi penali deve sentire e vedere, non solo sapere. Ma qualche dubbio rimane: che la pubblicità del giudizio debba talvolta cedere ai diritti di *privacy* è testimoniato dall'art. 472 comma 2 c.p.p.; e fa una certa impressione pensare che una video-intercettazione domestica possa liberamente circolare in rete per il solo fatto che su di essa è stato apposto il timbro "prova penale".

8. Intercettazioni e riservatezza

Se le intercettazioni vengono prese in considerazione unicamente nella loro dimensione di strumento che attenta alla riservatezza di chi viene intercettato (e delle persone di cui si parla), i limiti costituzionali, come è ovvio, si attenuano fin quasi a sparire. La riservatezza è un diritto che entra inevitabilmente in rotta di collisione con l'indagine e il processo penale: il compito degli inquirenti è esattamente quello di frugare nella vita privata dei potenziali autori di un reato, i quali non c'è dubbio che avrebbero interesse a mantenere riservata la notizia che amano dedicarsi all'usura o alla pedofilia. In questa ricerca, *è* inoltre fisiologico che gli inquirenti apprendano anche notizie attinenti alla vita privata dell'imputato che nulla hanno a che vedere con il reato per cui si indaga: ed è fisiologico che emergano anche notizie attinenti alla vita privata di soggetti del tutto estranei ai fatti. Il fenomeno è molto evidente nel caso delle intercettazioni, ma può

ovviamente manifestarsi anche nel corso di una perquisizione (tanto più se si tratta di una perquisizione *online* mediante captatore informatico) o quando si acquisisce una testimonianza.

Questo naturalmente non significa che il legislatore abbia mano libera nel calibrare i rapporti tra il rispetto delle esigenze di prevenzione e di accertamento dei fatti di reato e il sacrificio che ne può derivare ai diritti dei cittadini alla loro riservatezza (e, prima ancora, alla segretezza delle comunicazioni e all'intimità domiciliare). Gli artt. 14 e 15 Cost., da questo punto di vista, non aiutano, perché impongono la previsione di casi, modi e garanzie ma non dicono in che misura – cioè fino a che punto – l'intimità delle comunicazioni e del domicilio possono essere sacrificati sull'altare della giustizia penale. La stella polare normativa è contenuta nell'art. 8 della Convenzione europea dei diritti dell'uomo, che tollera gli attentati alla vita privata delle persone per esigenze di giustizia solo se «necessari in una società democratica». L'*explicit* ("in una società democratica") invita il legislatore a un'attenta ponderazione dei valori in gioco: la sorveglianza elettronica non si può spingere – neppure per contrastare la più efferata criminalità – fino a minare le fondamenta democratiche dello Stato. Il concetto, alquanto ovvio, era stato ribadito dal Parlamento Europeo in una Dichiarazione ufficiale del 1998 che muoveva da un'ipotesi estrema: nessun dubbio che «l'intercettazione di tutte le comunicazioni rappresenterebbe la migliore protezione contro la criminalità organizzata», ma una simile ricetta normativa «sarebbe contraria all'art. 8 Conv. eur.», perché «un sistema dei servizi d'informazione che captasse qualunque comunicazione costituirebbe comunque una violazione del principio di proporzionalità». Da quest'angolo visuale, suscita più di una perplessità la disciplina recentemente approvata delle intercettazioni effettuate mediante captatore informatico: l'impressione è che il legislatore abbia sottovalutato i devastanti pregiudizi che possono venire arrecati alla *privacy* delle persone che fanno uso – o entrano nel raggio d'azione – del dispositivo informaticamente modificato.

9. Intercettazioni e trattamento dei dati personali

Che la riservatezza sia un valore tendenzialmente recessivo rispetto alle esigenze della giustizia penale è testimoniato dallo stesso d.lgs. n. 51 del 2018, attuativo della Direttiva UE 680/2016, che sottrae al controllo del Garante il trattamento dei dati effettuato da giudici e pubblici ministeri (art. 37 comma 6) e consente di limitare o addirittura escludere i diritti dei titolari dei dati trattati per non compromettere il buon esito delle attività di indagine, accertamento e perseguimento di reati (art. 14 comma 2). In materia di intercettazioni, le ricadute del decreto legislativo appaiono dunque, in prospettiva, assai modeste. Come è già

stato esattamente notato da Andrea Zampini, un'informativa indirizzata all'indagato – nella sua veste di titolare dei dati trattati – sarebbe tanto deleteria a intercettazioni in corso quanto sostanzialmente inutile a deposito avvenuto (quando cioè l'indagato, avendo preso conoscenza delle comunicazioni intercettate, può esercitare il diritto alla cancellazione del dato personale ricorrendo alla procedura giurisdizionale di cui all'art. 269 comma 2 c.p.p.). Potrebbe invece svolgere una funzione preziosa l'invio dell'informativa ai terzi estranei che siano rimasti impigliati nella rete dell'intercettazione, i quali spesso non sospettano neppure di essere entrati nel mirino degli inquirenti (oppure di essere stati l'oggetto di colloqui intercettati) e – se venissero informati – potrebbero far valere anch'essi il diritto alla distruzione del materiale "non necessario" al processo. Sembra tuttavia improbabile che informative del genere saranno inviate, considerate anche le dimensioni gigantesche che può assumere un'attività captativa. Di un "avviso di avvenuta intercettazione" si discute dai tempi del disegno di legge Mastella del 2006: ma *è una* proposta di riforma che si è sempre arenata nelle secche di un rapporto costi/benefici eccessivamente sbilanciato sul primo versante.

10. Processo penale e riservatezza: lesioni inevitabili e lesioni gratuite

In ogni caso, se l'incombente istruttorio è rispettoso delle condizioni di legge, la *prima* lesione della riservatezza, quella contestuale al compimento dell'atto, è ovviamente legittima anche se inutile in chiave accertativa (nel corso di un'intercettazione si sentono descrivere le abitudini sessuali di una persona estranea ai fatti per cui si indaga; nel corso di una perquisizione si scopre che la moglie dell'indagato assume determinati medicinali ecc.). Il problema sono le lesioni *successive*, quelle che si consumano con l'uso della notizia riservata nel processo o tramite la pubblicazione dell'atto processuale. Qui il criterio-guida dovrebbe essere quello della rilevanza probatoria, variamente e alquanto confusamente declinato (rilevanza, non irrilevanza) dalle disposizioni codicistiche in materia di *screening* delle intercettazioni utilizzabili (l'art. 472 comma 2 c.p.p., nel limitare la pubblicità dell'udienza, allude invece alle notizie concernenti «fatti che non costituiscono oggetto dell'imputazione», dettando un criterio perfino troppo sbilanciato in favore della *privacy*). Le notizie private apprese nel corso dell'indagine che non servono al giudice per decidere dovrebbero rimanere segrete, perché la violazione della riservatezza sarebbe – a questo punto – consapevolmente gratuita e ingiustificata.

Due brevissime considerazioni su questo tema. La prima è che il criterio della rilevanza per il processo non va sopravvalutato in chiave di tutela della riservatezza, perché è un criterio molto più difficile da maneggiare e molto meno se-

lettivo di quanto possa apparire (basti pensare che sono oggetto di prova anche i fatti che si riferiscono alla determinazione della pena, e tra i fatti rilevanti per la determinazione della pena rientrano anche le condizioni di vita individuale e familiare dell'imputato). All'indubbia ma non decisiva rilevanza processuale di una comunicazione intercettata potrebbe corrispondere, ad esempio, una lesione gravissima della riservatezza dei soggetti coinvolti nelle attività di ascolto: così come, al contrario, nel corso dell'indagine potrebbero emergere notizie processualmente irrilevanti che sarebbe inopportuno, nell'interesse della collettività, consegnare all'oblio per ragioni di tutela della *privacy*.

La seconda considerazione riguarda il meccanismo di selezione delle intercettazioni rilevanti introdotto dalla "riforma Bonafede". Con il d.lgs. 29 dicembre 2017, n. 216 (che in questa parte non ha mai trovato attuazione) il legislatore aveva raccolto un annoso invito dottrinale: il segreto sulle comunicazioni intercettate veniva finalmente mantenuto fino alla conclusione della procedura di stralcio, nonostante l'avvenuta *discovery* dei materiali captati a beneficio della difesa. Il d.l. 30 dicembre 2019, n. 161, conv. nella legge 28 febbraio 2020, n. 7, ha inopportunamente innestato la retromarcia, benché qualcuno ritenga che la regola sia sopravvissuta, pur malconcia e sgrammaticata, alle interpolazioni legislative. Sul punto non si può che auspicare un nuovo deciso mutamento di rotta. Anche il più virtuoso rituale di esclusione dei materiali irrilevanti incontra, tuttavia, un grave limite: la mancanza, nel processo penale, di un soggetto istituzionalmente preposto a tutelare le ragioni dei terzi che siano stati occasionalmente coinvolti nelle operazioni di ascolto. Periodicamente si affaccia l'idea di coinvolgere nella procedura selettiva una sorta di "difensore della *privacy*": ma anche questo proposito – nobile ma costoso come quello di introdurre l'avviso di avvenuta intercettazione – *è probabilmente* destinato a rimanere nel libro dei sogni.

Federica Resta[1]

Pubblicità dei provvedimenti giurisdizionali e *privacy*

Sommario: 1. La disciplina applicabile. – 2. La *ratio* della disciplina, dal dibattito parlamentare del 2003 al d.lgs. 101 del 2018. – 3. La tenuta della disciplina vigente nel contesto attuale. – 3.1. L'estensione pretoria dei casi di oscuramento obbligatorio. – 3.2. L'anonimizzazione come regola? – 3.3. Cautele intermedie.

1. La disciplina applicabile

Il bilanciamento tra principio di pubblicità dei provvedimenti giurisdizionali e la tutela dei dati personali in essi contenuti va valutata essenzialmente alla luce degli artt. 51 e 52 del d.lgs. 30 giugno 2003, n. 196 e s.m.i. (*infra*: Codice), che disciplinano l'"informatica giuridica"[2]. Essa è concepita quale trattamento (retto da regime speciale) "necessario per adempiere un obbligo legale o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri", come recita il titolo della parte II del Codice al cui interno sono collocate tali disposizioni.

I tratti essenziali della disciplina – sostanzialmente invariata rispetto a quella previgente – sono i seguenti.

Le sentenze e le altre decisioni giudiziali, ai sensi dell'art. 51, comma 2, del Codice, "sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete *Internet*, osservando le cautele previste" nell'art. 52 tale deve intendersi il riferimento alle cautele previste dal capo in esame, relative ai casi di oscuramento obbligatorio (previsto *ex lege)* o eventuale (su istanza di parte o disposto officioso del giudice).

La possibilità di accedere alle sentenze e alle altre decisioni dell'autorità giudiziaria "di ogni ordine e grado" non è qui circoscritta ai soggetti portatori di uno

---

[1] Le opinioni contenute in questo contributo sono espresse dall'autrice a titolo esclusivamente personale e non impegnano in alcun modo l'Autorità di appartenenza.

[2] Nozione in parte inadeguata – come rilevato in dottrina – anche perché la relativa disciplina si riferisce prevalentemente all'informatica giudiziaria. In ogni caso, il termine "informatica" andrebbe in questo caso inteso nel suo significato originario, derivante dalla crasi tra "informazione" e "automatica", utilizzato per la prima volta nel 1962 da P. Dreyfus.

specifico interesse, ma estesa senza particolari limitazioni, in linea con il principio di pubblicità del giudizio e del suo atto conclusivo. Infatti, diversamente dalla disciplina dell'accessibilità ai dati identificativi delle questioni pendenti – i quali, ai sensi del comma 1 dello stesso art. 51, "sono resi accessibili *a chi vi abbia interesse"* anche mediante reti di comunicazione elettronica, ivi compreso il sito istituzionale della medesima autorità nella rete *Internet*" –, per le sentenze e per le altre decisioni dell'autorità giudiziaria mancano analoghe limitazioni.

In linea generale, dunque, le sentenze e gli altri provvedimenti giurisdizionali possono essere diffusi, anche attraverso il sito istituzionale *Internet*, nel loro *testo integrale*, salvo l'oscuramento delle generalità e degli altri dati identificativi sia stato disposto dal giudice d'ufficio, su istanza di parte o sia previsto dalla legge nei casi specifici di cui all'art. 52, c. 5. Infatti, al di fuori di tali casi, ai sensi del comma 7 dell'art. 52, "è ammessa la *diffusione in ogni forma* del contenuto *anche integrale* di sentenze e di altri provvedimenti giurisdizionali".

L'art. 52 definisce i casi nei quali è garantito il diritto all'anonimato delle parti (e, in alcuni casi, anche dei terzi).

Il primo riguarda l'oscuramento eventuale, disposto su istanza di parte o *jussu judicis*. Con riguardo al primo caso, sussistendo *motivi legittimi*[3], l'interessato

---

[3] Sul punto, di recente, Cass. civ., Sez. V, Ord. 7 agosto 2020, n. 16807, si sofferma sulle condizioni che devono essere soddisfatte per ottenere l'omissione delle generalità e degli altri dati identificativi in caso di pubblicazione di un provvedimento giurisdizionale avanzata, ai sensi dell'art. 52, comma 1, del Codice. Dopo aver ribadito che tale pretesa può essere avanzata dalla sola persona fisica che sia parte del procedimento, la Corte ritiene che locuzione "motivi legittimi", in assenza di più puntuale indicazione del legislatore, vada apprezzata « come sinonimo di "motivi opportuni": donde la particolare ampiezza, opportunamente non predeterminata dal legislatore all'interno di schemi rigidi, delle ragioni che possono essere addotte a sostegno della richiesta che qui interessa, fermo restando che l'accoglimento della richiesta medesima interverrà ogniqualvolta l'autorità giudiziaria ravviserà un equilibrato bilanciamento tra le esigenze di riservatezza del singolo e il principio della generale conoscibilità dei provvedimenti giurisdizionali e del contenuto integrale delle sentenze, quale strumento di democrazia e di informazione giuridica. In tal senso, interessanti indicazioni conformi si traggono dalle linee guida dettate dal Garante della privacy il 2 dicembre 2010, "in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica", pubblicate sulla G.U. n. 2 del 4 gennaio 2011, in cui al punto 3., con specifico riferimento alla c.d. "procedura di anonimizzazione dei provvedimenti giurisdizionali" di cui all'art. 52, commi da 1 a 4, del d.lgs. n. 196/2003, si indicano possibili "motivi legittimi", in grado di fondare la relativa richiesta (ovvero di indurre l'A.G. a provvedere d'ufficio), nella "particolare natura dei dati contenuti nel provvedimento (ad esempio, dati sensibili)", ovvero nella "delicatezza della vicenda oggetto del giudizio" (Cass. pen. 13 marzo 2017, n. 11959)». Nel caso di specie, non ricorrendo una di tali ipotesi ed essendosi le parti limitate a richiedere l'oscuramento delle generalità e degli altri dati identificativi ad essi riconducibili "avendone motivo legittimo", senza tuttavia esternare il medesimo, l'istanza non è stata accolta. V. anche Cass. civ., Sez. V,

(non solo, quindi, la parte del giudizio) può chiedere, prima della definizione del relativo grado di giudizio, che sull'originale della sentenza o del provvedimento sia apposta un'annotazione volta a precludere, appunto in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento. Il nuovo testo ha qui soppresso il riferimento previgente alla finalità di informazione giuridica sottesa alla pubblicazione su riviste giuridiche, che aveva generato dubbi in ordine all'applicabilità di tale disciplina alla divulgazione delle sentenze da parte della stessa a.g.

L'autorità giudiziaria, del resto, può disporre *d'ufficio* l'anonimizzazione a tutela dei diritti o della dignità degli interessati (art. 52, c. 2, ultimo periodo). Secondo quanto indicato con decreto n. 178 del 2016 del Primo Presidente della Corte suprema di cassazione, uno dei parametri per valutare la necessità di anonimizzare d'ufficio (eliminando le generalità) è la ricorrenza, nel provvedimento, di dati "sensibili" (come allora definiti dall'art. 4, comma 1, lett. d) del d.lgs. n. 196 del 2003).

In altri casi l'anonimizzazione è obbligatoria (e non rimessa, dunque, all'istanza di parte o ai poteri officiosi del giudice), in quanto prevista *ex lege*, relativamente ai dati comunque idonei a identificare minori; ai dati inerenti vittime di delitti sessuali o i dati delle parti di procedimenti inerenti rapporti di famiglia o stato delle persone (art. 52, c. 5). Lo stesso decreto identifica, in maniera puntuale, i casi in esame oltre che nei procedimenti civili inerenti minori, rapporti di famiglia e stato delle persone, nei procedimenti penali per reati contro la famiglia (artt. da 556 a 574-*bis* c.p.), per "reati di cui agli artt. 414-*bis* e 416, settimo comma, c.p., retai di cui all'art. 591 c.p., reati di cui agli artt. da 600-*bis* a 600-*octies* e da 609-*bis* a 609-*undecies* c.p., reati di cui all'art. 643 c.p., di cui all'art. 734-*bis* c.p., reati in tema di prostituzione, di interruzione volontaria della gravidanza, di procreazione medicalmente assistita e reati commessi in danno di minorenni", con la precisazione che in tali casi (come del resto prescrive l'art. 52, c.5) "l'oscuramento deve riguardare non solo i dati identificativi dell'interessato, ma ogni altro dato, anche relativo a terzi, tramite il quale si possa risalire anche direttamente alla sua identità".

---

23 dicembre 2019, n. 34275,che ha rigettato l'istanza avanzata *ex* art. 52 del d.lgs. 30 giugno 2003, n. 196, come modificato dall'art. 3, comma 2, lett. c), n. 1), del d.lgs. 10 agosto 2018, n. 101, dalla controricorrente – società nei confronti della quale era stato adottato un atto di accertamento e rettifica, nonché un provvedimento di irrogazione di sanzioni – atteso che detta società non aveva neanche indicato quali fossero "i «motivi legittimi» che giustificherebbero l'adozione del provvedimento invocato, né i dati personali riguardano una persona offesa da atti di violenza sessuale, ovvero minori o comunque parti di procedimenti in materia di rapporti di famiglia o di stato delle persone ai sensi dell'art. 52, comma 5, del d.lgs. n. 196 del 2003.

2. La ratio della disciplina, dal dibattito parlamentare del 2003 al d.lgs. 101 del 2018

Quella su descritta è una disciplina fondata sul bilanciamento tra riservatezza delle parti processuali (e dei terzi) e pubblicità del processo, funzionale tanto alla garanzia dei diritti della difesa e del contraddittorio (pubblicità endoprocessuale), quanto al "controllo della pubblica opinione" sull'esercizio del potere giurisdizionale (essendo la giustizia amministrata in nome del popolo, ai sensi dell'art. 101, I c., Cost.: cfr. Corte cost., *ex plurimis*, sent. 27 luglio 1992, n. 373 e dovendo tutti i provvedimenti giurisdizionali essere necessariamente motivati: art. 111, sesto comma[4]).

Tali norme mirano infatti – come affermava la Relazione illustrativa del Codice del 2003 – ad agevolare lo sviluppo dell'informatica giuridica nel rispetto dei principi in materia di protezione dei dati personali", favorendo "la conoscibilità dei dati identificativi (…) delle decisioni giudiziarie adottate mediante reti di comunicazioni elettronica, anche attraverso il sito *Internet* dell'autorità giudiziaria".

*L*a disciplina in esame attuava quindi il criterio direttivo di cui all'art. 1, comma 1, lettera l), della legge di delegazione (da cui sarebbe stato poi emanato il d.lgs. 196 del 2003), inerente l'obiettivo di "favorire lo sviluppo dell'informatica giuridica", in conformità, peraltro, a direttive sovranazionali quali ad esempio le Raccomandazioni del Consiglio d'Europa R (2001)2 e R (2001)3", tese a impegnare gli Stati membri nell'adozione di ogni misura necessaria a favorire l'accesso dei cittadini agli archivi legislativi e giurisprudenziali mediante l'uso delle tecnologie dell'informazione.

Il parere parlamentare sullo schema di Codice aveva, del resto, indotto il Governo ad ampliare i margini di pubblicità delle sentenze e degli altri provvedimenti giurisdizionali, ulteriormente rispetto a quanto previsto dal testo originario, suggerendo una "generale riconsiderazione" dell'art. 52, c. 1, "cosicché – ferma restando la condivisa previsione della facoltà per l'interessato di garantire il proprio anonimato in occasione della divulgazione di provvedimenti giudiziari che lo riguardano, resti tuttavia opportunamente garantita la funzione di pubblicità, nell'interesse dei terzi" (parere approvato dalla 2^ Commissione del Senato nella seduta del 24.6.2003, rel. Consolo).

Il testo originario dello schema di decreto prevedeva, in particolare, che l'oscuramento richiesto dall'interessato operasse "*in caso di diffusione della sentenza o provvedimento in qualsiasi forma, anche su riviste giuridiche*". Tale for-

[4] Interessanti, soprattutto a questo proposito, le considerazioni svolte da G. Grasso, *Il trattamento dei dati di carattere personale e la riproduzione dei provvedimenti "giudiziari"*, in *Foro it*., 2018, V, 349. V. anche A. Centonze, *Il diritto alla riservatezza e la tutela dei dati personali nei provvedimenti giurisdizionali della Corte di Cassazione*, in www.giustiziainsieme.it.

mulazione aveva suscitato il timore che l'oscuramento richiesto dall'interessato operasse anche al di là del settore della ricerca o documentazione giuridica, precludendo tout court la conoscenza dell'identità delle parti anche, ad esempio, a fini giornalistici o comunque *lato sensu* informativi.

Per questo, la versione finale del d.lgs. 196 del 2003 aveva poi previsto che l'oscuramento – disposto su istanza di parte o e*x officio* – operasse in caso di "riproduzione della sentenza o provvedimento in qualsiasi forma, per finalità di informazione giuridica", dunque chiarendo che la preclusione operasse solo nelle ipotesi di pubblicazione per finalità di informazione giuridica, rimettendo invece l'ammissibilità o meno della pubblicazione integrale per fini diversi, alla disciplina dei diversi settori interessati (es. quella del trattamento per fini di giornalismo o la redazione della sentenza ai fini processuali, come precisato sia dalla circolare del 17 gennaio 2006 del Primo Presidente della Corte di Cassazione, sia dal § 1.2 delle Linee guida del Garante del 2010 proprio sull'informatica giuridica).

Nel dibattito parlamentare si era, in particolare, richiamato il timore che la versione originaria del decreto inficiasse " *il principio della conoscibilità generale dei procedimenti giurisdizionali e del contenuto integrale delle sentenze definitive anche di condanna, che deve essere comunque assicurato*" (sen. Luigi Bobbio).

Analogamente, il Sen. Bucciero riteneva necessario assicurare – pur nel necessario contemperamento degli interessi – la più ampia pubblicità del contenuto delle sentenze definitive, paventando il timore che "*altrimenti un'enfasi eccessiva delle ricordate esigenze di tutela della riservatezza possa dar luogo a gravi distorsioni"*.

La formulazione poi adottata dal d.lgs. 196 del 2003 e le ragioni che ne sono alla base hanno anche fondato una lettura della norma, vigente sino al 2018, come volta a limitare la possibilità di oscuramento (disposta su istanza di parte o *ex officio*), alle sole sentenze diffuse su siti di ricerca e documentazione giuridica diversi da quelli dell'a.g., che invece avrebbero potuto pubblicare integralmente i provvedimenti in quanto lo avrebbero fatto non già per fini di informazione giuridica, ma in ossequio al dovere di pubblicazione della sentenza previsto dalle norme processuali (che sono, infatti, espressamente fatte salve dagli artt. 51 e 52 del Codice, con un'apposita clausola di riserva).

Il sito dell'a.g. sarebbe stato dunque una sorta di "cancelleria virtuale", nella quale non sarebbe stato possibile oscuramento alcuno, esattamente come – lo ribadiva anche la circolare citata del Primo presidente della Cassazione – nella redazione della sentenza non potrebbe mai ammettersi l'indicazione delle sole iniziali per le parti o i terzi[5].

[5] Ufficio del Massimario della Suprema Corte di Cassazione, *Corte di Cassazione e tutela della privacy: l'"oscuramento" dei dati identificativi nelle sentenze*, in www.cortedicassazione.it; M. Mar-

Questa lettura, tuttavia, avrebbe indebolito la tutela della riservatezza degli interessati consentendo l'esistenza di almeno un sito (quello dell'a.g.) ove persino chi lo avesse espressamente richiesto, non avrebbe potuto beneficiare dell'oscuramento, così vanificando di fatto lo stesso istituto dell'anonimizzazione dei provvedimenti giurisdizionali.

Il Garante, nell'applicazione del testo previgente dell'art. 52 – e in particolare con le Linee guida del 2010 – ha adottato la lettura più garantista (ritenendo dunque anche il sito dell'a.g. assoggettabile alla disciplina sull'oscuramento obbligatorio od eventuale), ferma restando la legittimità della pubblicazione integrale delle sentenze *on-line* al di fuori dei casi di oscuramento disposto od obbligatorio.

La versione dell'art. 52, c.1 novellata dal d.lgs. 10 agosto 2018, n. 101, oggi vigente, ha fugato ogni dubbio in proposito, sopprimendo il richiamo (contenuto nel testo del 2003) alla finalità di informatica giuridica sottesa alla riproduzione della sentenza, così da conferire alla disciplina in esame una valenza applicativa la più ampia possibile.

Ad oggi, dunque, può confermarsi che la disciplina degli artt. 51-52 del Codice sancisce il principio generale (enunciato dal 52, c. 7) della pubblicazione integrale (anche *on-line*) delle sentenze quale regola, appunto, generale e ordinaria, salve le eccezioni previste dai primi cinque commi, inerenti l'oscuramento eventuale (disposto su istanza di parte o d'ufficio) o quello obbligatorio, sancito *ex lege* al comma 5, per le vittime di delitti sessuali o per procedimenti in materia di famiglia e stato delle persone, nonché per ogni dato idoneo a identificare il minore comunque coinvolto nel giudizio (in tal senso v. anche le citate Linee-guida del Garante e la circolare del Primo Presidente della Cassazione).

Principio, questo, ribadito anche dall'art. 51, c. 2 del Codice, che impone di garantire l'accessibilità *on-line*, anche mediante il sito dell'a.g., delle sentenze, sia pur con le cautele relative appunto a quei casi di oscuramento eventuale o *ex lege* già citati.

Se, infatti, l'accessibilità non equivale di per sé a pubblicazione, in tal senso deve invece essere letto l'art. 51, c.2, in combinato disposto con l'art. 52, c. 7 (che parla di pubblicazione, dunque ad accesso ampio e non limitato) e con il generale principio di pubblicità del processo e del suo provvedimento conclusivo.

Principio ben espresso, in particolare, dall'art. 744 c.p.c, sul dovere del cancelliere di "spedire a chiunque ne faccia istanza" (non a chiunque vi abbia interesse), eccettuati i casi determinati dalla legge, "le copie e gli estratti degli atti giudiziali da essi detenuti, sotto pena dei danni e delle spese".

CHETTI, *sub art. 52* in C. M. BIANCA – F.D. BUSNELLI (a cura di), *La protezione dei dati personali*, Padova, 2007, 966 ss.).

Del resto, in favore della non selettività dell'accesso alle sentenze depone anche il diverso tenore testuale dell'art. 51, c. 2, che non circoscrive in alcun modo l'accessibilità di tali provvedimenti, a differenza, ad esempio, di quanto disposto dal comma 1, che consente soltanto "a chi vi abbia interesse" l'accesso ai "dati identificativi delle questioni pendenti dinanzi all'a.g.". Tale diverso regime si fonda sul differente grado di definitività e completezza dell'accertamento giudiziale (tendenzialmente pieno per le sentenze, sia pur non irrevocabili; parziale nel caso di procedimenti non ancora conclusi). Tale duplice regime è stato del resto confermato, pochi anni dopo il Codice, dall'art. 56 del Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82) e dalle novelle successive[6].

La novità più rilevante del d.lgs. 101 del 2018 concerne, tuttavia, l'espressa soggezione, ai sensi dell'art. 166, c.2, a sanzione amministrativa pecuniaria (con le sanzioni definite in giurisprudenza punitive in senso convenzionale,[7] suscettibili di giungere fino a 20_milioni di euro o al 4% del fatturato) dell'inadempimento degli obblighi di anonimizzazione per previsione di legge o decisione giudiziale.

3. La tenuta della disciplina vigente nel contesto attuale

La scelta del legislatore del 2018, di lasciare sostanzialmente invariata la disciplina in esame (salvo, come detto, l'espressa estensione del suo ambito applicativo senza limiti teleologici e l'aggiornamento dei riferimenti al collegio arbitrale per i lavori pubblici che, pure, è assoggettato ad essa) può ritenersi probabilmente una scelta non del tutto obbligata e forse suscettibile di alternative maggiormente conformi all'evoluzione registratasi in materia.

Sotto il primo profilo, infatti, l'assenza, in legge di delegazione, di espressi criteri di delega sul punto non avrebbe certo ostato a un pieno adeguamento

[6] Inoltre, anche la disposizione transitoria del Codice del 2003 (art. 181, c. 5 d.lgs. 196 del 2003) volta a regolare l'applicazione della disciplina di cui agli artt. 51 e 52 alle sentenze già emesse alla data della sua entrata in vigore, limitava la possibilità di oscuramento ai soli casi nei quali l'interessato avesse fatto apposita richiesta, con ciò confermando come l'anonimizzazione rappresenti un'eccezione al principio generale della pubblicità delle decisioni giudiziarie. Principio cui, del resto, si conformano anche altri ordinamenti europei, nonché la stessa Cedu, nei cui siti istituzionali le sentenze sono generalmente pubblicate in forma integrale (la Corte di Giustizia ha iniziato ad anonimizzare soltanto da un anno). E se è certamente vero che pubblicità della sentenza non implica necessariamente sua pubblicazione *on-line*, è altrettanto vero che la disciplina vigente sembra accogliere tale principio di diritto, ben espresso dalla giurisprudenza di Cassazione, già richiamata e costante nel subordinare l'oscuramento su istanza di parte a motivi, appunto, legittimi.

[7] Trib. Palermo, sez. I civ., sent. 18 luglio 2019, n. 3563.

della disciplina in esame ai principi (di minimizzazione, proporzionalità ecc.) sanciti dal Regolamento (UE) 2016/679, ricorrendo al criterio del doppio parametro di costituzionalità da seguire nell'esercizio del potere normativo delegato, valorizzando dunque la cogenza del parametro europeo cui adeguare, appunto, l'ordinamento.

La delega per il d.lgs. 101 era, infatti, come noto e come sempre in questi casi, sostanzialmente estrinseca, recante pochi e lati criteri direttivi, tali da configurare una sufficiente discrezionalità nell'esercizio governativo della delega, ai limiti delle deleghe di riordino e riassetto. Del resto, le deleghe per adeguamento/trasposizione di norme europee devono ispirarsi, tra gli altri, al criterio di migliore adattamento dell'ordinamento interno alla disciplina Ue e certamente ciò avrebbe implicato una riflessione più ampia sulla disciplina della pubblicità delle sentenze (per riferimenti alla questione del doppio parametro, europeo e interno, di costituzionalità, cui conformare l'esercizio del potere delegato rispetto ai principi e criteri direttivi, vds. C. Cost. sent. 29 ottobre 2015, n. 210).

Sotto il secondo profilo, la pervasività della rete, la viralità della condivisione dei contenuti on line e in particolare sui social, hanno evidenziato i rischi cui la disciplina vigente – improntata alla pubblicità di tutti i provvedimenti giudiziari salvo i casi di anonimizzazione *ex lege o jussu judicis* – espone la *privacy*, ben più di quanto potesse avvenire nel 2003, ovvero alla data di emanazione del Codice nel testo originario.

Tali considerazioni avevano fatto registrare, già sotto il vigore del Codice ante-dlgs 101 del 2018, alcune interpretazioni evolutivo-adeguatrici del regime di pubblicità delle sentenze, di cui si dirà di seguito.

3.1. L'estensione pretoria dei casi di oscuramento obbligatorio

Tra le interpretazioni adeguatrici rese della disciplina delle sentenze on line, vi è quella dei casi di oscuramento obbligatorio, tra i quali la sent. della I sezione civile della Corte di Cassazione del 20 maggio 2016, n. 10510, ha incluso anche i provvedimenti contenenti dati idonei a rivelare lo stato di salute, in ragione dell'espresso divieto di pubblicazione sancito (allora dall'art. 22, c. 8, oggi dall'art. 2-*septies*, c. 8 del Codice, con l'ulteriore aggiunta dei dati genetici e biometrici) rispetto alla disciplina generale del trattamento per fini di pubblico interesse.

Si è trattato di un'interpretazione assai avanzata – e recepita peraltro subito dal decreto del Presidente del Consiglio di Stato n. 134 del 22 maggio 2020 recante regole tecnico-operative per l'attuazione del processo amministrativo telematico – in quanto tale divieto di divulgazione di dati sanitari non è in alcun

modo richiamato dagli artt. 51-52 del Codice. Pertanto, prima di quella sentenza di Cassazione tale divieto di divulgazione dei dati sanitari non era ritenuto applicabile alla disciplina delle sentenze on line, rispetto al primo speciale e dunque assorbente.

Tuttavia, una volta consolidato quest'orientamento, il Garante, con il parere n. 88 del 19 maggio 2020 sul citato decreto del Presidente del Consiglio di Stato, ha espressamente sostenuto la legittimità di tale interpretazione, ritenendo dunque necessario l'oscuramento di tali dati, unitamente a quelli genetici e biometrici, ora accomunati, nel divieto di pubblicazione generale, ai dati sanitari dall'art. 2-*septies* c. 8, del Codice.

3.2. L'anonimizzazione come regola?

La consapevolezza dei rischi cui la viralità della rete espone la persona i cui dati siano contenuti in provvedimenti giudiziari, ha indotto a ipotizzare l'anonimizzazione "di *default*" di tutte le sentenze riprodotte *on line* (tale auspicio è prospettato anche dal Presidente del Garante, Antonello Soro, nella nota al Primo Presidente della Corte suprema di Cassazione, del 6 ottobre 2014).

Tale previsione (sostanzialmente opposta a quella attuale e analoga alla prassi dei sistemi francese e tedesco) era contenuta nello schema di decreto legislativo correttivo del Codice dell'amministrazione digitale, su cui il Garante si è pronunciato con parere n. 255 del 9 giugno 2016, ma che è stata poi soppressa su indicazione del Consiglio di Stato, in ragione dell'assenza di specifici criteri di delega sul punto[8].

---

[8] Il parere del Garante sul punto osservava: "L'art. 46 dello schema nel sostituire il comma, 2-*bis* dell'art. 56 del CAD, prevede espressamente che "alla pubblicazione delle sentenze e delle altre decisioni di cui al comma 2 si provvede nel rispetto di quanto previsto all'articolo 52 del decreto legislativo n. 196 del 2003". Questa disposizione deve essere letta in combinato disposto con quanto previsto dall'art. 62, comma 5, lett. b) del d.lgs. di modifica del CAD. L'art. 62 infatti reca "disposizioni di coordinamento" dello schema di decreto e prevede anche la modifica dell'art. 52 del Codice, in particolare sopprimendo la necessità da parte dell'interessato di specificare i "motivi legittimi" per la richiesta di soppressione delle generalità in corso di giudizio e introducendo la possibilità di presentare tale richiesta successivamente alla pubblicazione della sentenza, anche al gestore del sito internet o all'editore della rivista giuridica, anche *on-line*, che abbia proceduto alla pubblicazione. L'articolo dispone, inoltre, l'anonimizzazione dei dati personali delle parti e di terzi, contenuti nelle sentenze adottate successivamente al 1° gennaio 2016, prima della loro pubblicazione. Al riguardo, considerato quanto osservato dal Consiglio di Stato, secondo cui l'introduzione nel CAD di nuove disposizioni in materia di tutela dei dati personali o in materia di pubblicazione dei provvedimenti dell'autorità giudiziaria sarebbe da considerare fuori delega, si prende atto, come riportato nel parere dell'11 maggio del citato Consiglio, dell'impegno dell'Amministrazione a

Non si tratterebbe però di una prospettiva oggi peregrina, se si considera che dopo l'entrata in vigore del Regolamento (UE) 2016/679 moltissimi ordinamenti (e finanche la stessa Corte di Giustizia) hanno disposto l'anonimizzazione d'ufficio delle copie delle sentenze da pubblicare *on line* (gli ordinamenti francese e tedesco anche prima della data di entrata in vigore del Regolamento 2016/679).

Naturalmente si dovrebbe tenere fermo il diverso regime di pubblicità dei provvedimenti giurisdizionali (o meglio di loro stralci) a fini giornalistici, soggetto ai canoni sanciti dalle regole deontologiche e, in particolare, dal criterio dell'essenzialità dell'informazione.

3.3. Cautele intermedie

Come già rappresentato dal Presidente Soro nella nota al Presidente Santacroce del 2014, pur nel vigore della disciplina vigente si potrebbe valutare di disporre (anche da parte delle stesse autorità giudiziarie e come, peraltro, dispone la Corte di Cassazione) la deindicizzazione dei provvedimenti giurisdizionali, in ragione del potenziale lesivo connesso alla indiscriminata reperibilità *on-line* delle pronunce. Se, infatti, è vero che l'interessato potrebbe rivolgersi allo stesso motore di ricerca per ottenere analogo risultato, è altresì vero che tale soluzione tecnica, pur non comportando in alcun modo una limitazione del principio della pubblicità della sentenza, consentirebbe quantomeno di contenere il pregiudizio derivante all'interessato da tale divulgazione. Analoga soluzione è, del resto, stata discussa per le Camere (a seguito della sentenza n. 21961 del 2011, della sezione I del Tribunale di Roma) in relazione all'esigenza di contemperamento

---

verificare la compatibilità di tale disposizione: "La Commissione speciale (…) ritiene di esprimere il proprio favorevole avviso sulla decisione, assunta dall'Amministrazione, di procedere a una nuova valutazione in merito alla compatibilità di quanto disposto dall'art. 62, comma 5, lettera b) del decreto – relativo alla "anonimizzazione" dei dati personali contenuti nelle sentenze e negli altri atti dell'autorità giudiziaria" – con i criteri di delega recati dall'art. 1 della legge n. 124 del 2015, "in vista di una eventuale espunzione" della disposizione de qua dall'articolato." Il Consiglio di Stato rappresenta il rischio che "la generalizzata "anonimizzazione" delle decisioni dell'autorità giudiziaria, svincolata da una valutazione caso per caso da parte degli organi giudicanti già prevista dalla vigente normativa, potrebbe comportare – come esposto nel parere interlocutorio in epigrafe – un "ingiustificato" appesantimento dell'attività amministrativa connessa con l'esercizio della funzione giurisdizionale, con conseguenti effetti negativi sull'efficacia e sulla speditezza della stessa.". Tuttavia, in proposito, il Garante rappresenta che l'appesantimento dell'attività potrebbe derivare più da una valutazione caso per caso dell'esigenza di anonimizzare, che dalla generalizzata anonimizzazione, anche perché le sentenze da anonimizzare verrebbero redatte seguendo opportune tecniche."

tra pubblicità dei lavori parlamentari (anch'essa costituzionalmente garantita *ex* art. 64) e riservatezza degli interessati, soprattutto riguardo alla pubblicazione in chiaro degli atti di sindacato ispettivo, non di rado recanti dati sensibili (ora "appartenenti a categorie particolari") e giudiziari di terzi.

Pro futuro (ovvero per i provvedimenti giurisdizionali di prossima emanazione), si potrebbe valutare di esercitare il potere di oscuramento d'ufficio con maggiore ampiezza, in considerazione del pregiudizio che deriva agli interessati dalla divulgazione in rete dei loro dati e, soprattutto, dalla loro reperibilità mediante motori di ricerca generalisti. L'elemento negativo di questa soluzione concerne l'onere di cui si grava il giudice rispetto a un bilanciamento che, forse, sarebbe preferibile venisse svolto *ex ante* dal legislatore.

Queste sono soluzioni perfettamente compatibili con il dettato normativo vigente, che tuttavia si potrebbe valutare di riformulare, prevedendo l'oscuramento d'ufficio di tutti i dati personali, in caso di pubblicazione per fini extraprocessuali (fermo restando, ovviamente, il diverso regime del giornalismo), anche in caso di diffusione sul sito istituzionale per fini di generica documentazione giurisprudenziale.

L'esigenza di consentire il sindacato pubblico sull'esercizio del potere giurisdizionale, infatti, non necessita della indicazione dei nomi delle parti, che nulla aggiunge alla "sostanza della decisione".

Tale soluzione dovrebbe valere, *a fortiori*, per quegli atti endoprocedimentali ulteriori quali ad esempio quelli funzionali alla composizione delle crisi da sovraindebitamento (del cui regime di pubblicità il Garante si è occupato più volte), per le quali la l. 3 del 2012 non prevede una specifica modalità di pubblicazione (rimettendo al giudice, ad esempio epr il piano, la valutazione delle forme "idonee"), ma che contengono spesso dati sulla salute o altri dati parimenti meritevoli, secondo l'ordinamento, di una tutela rafforzata.

A diversa soluzione potrebbe, invece giungersi, per l'accesso agli archivi anche telematici dei provvedimenti giurisdizionali, da parte degli esercenti le professioni forensi, che ben potrebbe mantenersi "aperto", in ragione della funzione svolta e delle conseguenti diverse esigenze conoscitive.

Alessandro Centonze

La protezione dei dati personali nei provvedimenti della Corte di Cassazione

Sommario: 1. La protezione dei dati personali e l'entrata in vigore del d.lgs. 30 giugno 2003, n. 196. – 2. La tutela dei dati personali nei provvedimenti della Corte di Cassazione. – 3. Segue: il settore civile. – 4. Segue: il settore penale. – 5. Gli interventi della Corte Costituzionale e la protezione dei dati personali nei provvedimenti giurisdizionali.

1. La protezione dei dati personali e l'entrata in vigore del d.lgs. 30 giugno 2003, n. 196

Nella cornice normativa che si è descritta nel paragrafo precedente, deve evidenziarsi che nell'ordinamento italiano il punto di partenza di ogni disamina sul tema della tutela dei dati personali nei provvedimenti giurisdizionali è rappresentato dal d.lgs. 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali»[1].

Questo testo legislativo, a sua volta, deve essere correlato alle norme del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riferimento al trattamento e alla libera circolazione dei dati personali, convenzionalmente noto, per la sua denominazione in lingua inglese, come *General Data Protection Regulation* ovvero con l'acronimo di GDPR.

Questa correlazione normativa si impone in conseguenza del fatto che l'entrata in vigore del Regolamento (UE) 2016/679, essendo direttamente applicabile in tutti gli Stati membri dell'Unione europea, a partire dal 25 maggio 2018, ha reso necessario l'adeguamento del preesistente "Codice in materia di protezio-

[1] Sulla rilevanza sistematica e sulla portata applicativa del "Codice in materia di protezione dei dati personali" si rinvia agli studi di G. Grasso, *Il trattamento dei dati di carattere personale e la riproduzione dei provvedimenti giudiziari*, in *Foro it.*, 2018, V, 349; F. Midiri, *Il diritto alla protezione dei dati personali. Regolazione e tutela*, Napoli, Torino, 2017; A. Pisapia, *La tutela per il trattamento e la protezione dei dati personali*, Torino, 2018; S. Scagliarini, *Il "nuovo" codice in materia di trattamento di dati personali. La normativa italiana dopo il d.lgs. 101/2018*, Torino, 2019.

ne dei dati personali"[2], introdotto nel nostro ordinamento giuridico con il d.lgs. n. 196 del 2003.

Si tratta, a ben vedere, di una vera e propria opera di adeguamento normativo, perché il legislatore italiano non ha abrogato il previgente "Codice in materia di protezione dei dati personali", provvedendo a una sua complessiva rivisitazione, realizzata mediante l'approvazione del 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)». Tale procedimento di rivisitazione del testo normativo preesistente è stato attuato mediante l'abrogazione delle disposizioni previgenti incompatibili con il Regolamento (UE) 2016/679 e il contestuale adeguamento del «Codice in materia di protezione dei dati personali», effettuato attraverso l'inserimento di nuove disposizioni o la modifica di quelle precedentemente vigenti.

All'esito di questo complesso procedimento di rivisitazione sistematica, il legislatore italiano ha articolato la materia della protezione dei dati personali in due distinti piani normativi, rispettivamente riguardanti il trattamento dei dati personali da parte degli organi di giustizia e la divulgazione all'esterno, per finalità di informazione e di informatica giuridica, delle pronunce giurisdizionali.

Al primo di questi piani normativi, riguardante il trattamento dei dati personali da parte degli organi di giustizia, è dedicato l'art. 2-*duodecies* del d.lgs. n. 196 del 2003, così come integrato dal d.lgs. n. 101 del 2018.

Questa disposizione, in particolare, stabilisce che, nella materia in esame, i «diritti e gli obblighi di cui agli artt. da 12 a 22 e 34 del Regolamento sono disciplinati nei limiti e con le modalità previste dalle disposizioni di legge o di regolamento che regolano tali procedimenti».

Nel quarto comma dell'art. 2-*duodecies*, inoltre, si precisa che i trattamenti dei dati personali effettuati per "ragioni di giustizia" sono quelli «correlati alla trattazione giudiziaria di affari e controversie», nonché quelli «effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonché i trattamenti svolti nell'ambito delle attività ispettive su uffici giudiziari [...]». Nel-

[2] Sul testo originario del "Codice in materia di protezione dei dati personali", conseguente all'approvazione del d.lgs. 30 giugno 2003, n. 196 e sulle complesse questioni ermeneutiche prodotte dalla sua entrata in vigore, si rinvia a Corte di Cassazione – Ufficio del Massimario e del Ruolo, *Corte di Cassazione e tutela della privacy: "l'oscuramento" dei dati identificativi nelle sentenze*, Relazione del 5 luglio 2005 redatta a cura di A. Giusti ed E. Calvanese.

lo stesso contesto normativo, si precisa anche che le "ragioni di giustizia" non ricorrono «per l'ordinaria attività amministrativo-gestionale di personale, mezzi, strutture, quando non è pregiudicata la segretezza di atti direttamente connessi alla trattazione giudiziaria di procedimenti».

Al secondo di questi piani normativi, riguardante la divulgazione all'esterno, per finalità di informazione e di informatica giuridica, del contenuto dei provvedimenti giurisdizionali, sono dedicate le norme degli artt. 51 e 52 del d.lgs. n. 196 del 2003, così come integrate dal d.lgs. n. 101 del 2018.

Gli artt. 51 e 52, quindi, costituiscono la piattaforma normativa indispensabile per inquadrare il tema del trattamento dei dati personali in materia di informazione e di informatica giuridica, cui si collega la questione delle limitazioni applicabili alla diffusione, integrale o parziale, delle pronunzie giudiziarie.

Più precisamente, l'art. 51 del «Codice in materia di protezione dei dati personali», che è rimasto immutato a seguito dell'entrata in vigore del d.lgs. n. 101 del 2018, disciplina la diffusione dei provvedimenti giudiziari, prevedendo, nel suo primo comma, che i «dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado sono resi accessibili a chi vi abbia interesse anche mediante reti di comunicazione elettronica, ivi compreso il sito istituzionale della medesima autorità nella rete Internet». Il secondo comma dell'art. 51, invece, stabilisce che le «sentenze e le altre decisioni dell'autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet, osservando le cautele previste dal presente capo».

Le cautele richiamate dal secondo comma dell'art. 51, a sua volta, sono disciplinate dal successivo art. 52, parzialmente modificato dal d.lgs. n. 101 del 2018, che individua i limiti alla diffusione del contenuto, integrale o parziale, delle sentenze e degli altri provvedimenti giurisdizionali. Tali limiti si applicano sia nelle ipotesi di divulgazione per finalità di informazione giuridica su riviste scientifiche o su supporti elettronici, sia in ogni altra ipotesi di riproduzione di pronunce giudiziarie, come nel caso della diffusione di notizie su organi di stampa.

2. La tutela dei dati personali nei provvedimenti della Corte di Cassazione

Dopo avere ricostruito la cornice normativa nella quale si inseriscono i temi del diritto alla riservatezza e della tutela dei dati personali, occorre passare a considerare le modalità con cui tale protezione viene garantita nei provvedimenti giurisdizionali, civili e penali, della Corte di Cassazione.

A tale problematica è dedicato il decreto del Primo Presidente della Corte di Cassazione 14 dicembre 2016, n. 178, dalla cui ricognizione occorre muovere per inquadrare la materia di cui ci stiamo occupando[3].

Occorre premettere che questo decreto mira ad assicurare la più ampia diffusione dei provvedimenti giurisdizionali, civili e penali, della Corte di Cassazione, che però deve essere garantita nel rispetto del diritto alla protezione dei dati personali dei soggetti processuali. A tali obiettivi ci si si riferisce espressamente nel preambolo del decreto presidenziale in esame, in cui si richiama «l'esigenza di assicurare la più ampia informazione in ordine alle decisioni della Corte di Cassazione nel rispetto del diritto alla protezione dei dati personali […] relativamente alla riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica»[4].

Allo scopo di assicurare il contemperamento di tali esigenze, nel decreto n. 178 del 2016, innanzitutto, il Primo Presidente della Corte di Cassazione sollecita l'attenzione dei collegi giudicanti – e in particolare dei presidenti e degli estensori dei provvedimenti giurisdizionali oggetto di potenziale diffusione esterna – sulla necessità o sull'eventualità di disporre l'oscuramento dei dati identificativi dei soggetti coinvolti in un procedimento di legittimità, civile o penale, con le modalità disciplinate dall'art. 52 del d.lgs. n. 196 del 2003[5].

Tale collaborazione, processuale e istituzionale, nella prospettiva auspicata dal decreto presidenziale in esame, si rende indispensabile, attesa «l'impossibilità di prevedere forme di controllo e di "oscuramento" standardizzate, in particolare con riferimento alle specifiche parti da anonimizzare nei singoli provvedimenti e all'individuazione dei procedimenti nei quali sono coinvolti minori non come parti, ma, ad esempio, come testimoni»[6].

In questo contesto, occorre distinguere le ipotesi in cui l'oscuramento dei dati personali di un soggetto processuale deve essere eseguito sulla base delle emergenze del caso concreto, previste dall'art. 52, comma 2, del d.lgs. n. 196 del 2003, dalle ipotesi in cui l'oscuramento dei dati personali deve essere eseguito obbligatoriamente, previste dall'art. 52, comma 5, del d.lgs. n. 196 del 2003.

Rientrano, in particolare, nel primo ambito normativo, connotato da discrezionalità, le ipotesi previste dall'art. 52, comma 2, del d.lgs. n. 196 del 2003, rilevanti «nei procedimenti civili e nei procedimenti penali concernenti "dati sensibi-

---

[3] Il decreto del Primo Presidente della Corte di Cassazione 14 dicembre 2016, n. 178 può essere consultato sul sito *www.cortedicassazione.it*, cui occorre rinviare per la sua lettura integrale.

[4] Si veda decreto del Primo Presidente della Corte di Cassazione 14 dicembre 2016, cit.

[5] Vedi *supra* paragrafo 2.

[6] Si veda decreto del Primo Presidente della Corte di Cassazione 14 dicembre 2016, cit.

li" […]», per i quali l'oscuramento dei dati personali «ha ad oggetto unicamente il nominativo dell'interessato […]»[7].

Rientrano, invece, nel secondo ambito, connotato da obbligatorietà, le ipotesi, previste dall'art. 52, comma 5, del d.lgs. n. 196 del 2003, rilevanti «nei procedimenti civili concernenti minori, rapporti di famiglia e stato delle persone, nonché nei procedimenti penali concernenti reati contro la famiglia (artt. da 556 a 574-*bis* cod. pen.), reati di cui agli artt. 414-*bis* e 416, settimo comma, cod. pen., reati di cui all'art. 591 cod. pen., reati di cui agli artt. da 600-*bis* a 600-*octies* e da 609-*bis* a 609-*undecies* cod. pen., reati di cui all'art. 643 cod. pen., reati di cui all'art. 734-*bis* cod. pen., reati in tema di prostituzione, reati in materia di interruzione volontaria della gravidanza, reati in materia di procreazione medicalmente assistita, e reati commessi da o in danno di minorenni […]»[8]. In queste ipotesi, secondo quanto previsto dal decreto in questione, l'oscuramento «deve riguardare non solo i dati identificativi dell'interessato, ma ogni altro dato, anche relativo a terzi, tramite il quale si possa risalire anche direttamente alla sua identità»[9].

Occorre, infine, evidenziare che, nella prospettiva collaborativa auspicata dal provvedimento presidenziale in esame, l'attività di selezione dei procedimenti oscurabili deve essere svolta dagli organi della Corte di Cassazione da cui transita il fascicolo processuale dopo la presentazione del ricorso, costituiti, come vedremo, dalle Cancellerie penali e civili; dagli Uffici per l'esame preliminare dei ricorsi, costituiti presso le sezioni civili e penali; dai collegi giudicanti ai quali il fascicolo è assegnato dopo la fissazione dell'udienza; dal magistrato estensore della sentenza; dall'Ufficio del Massimario e del Ruolo della Corte di Cassazione; dall'Ufficio C.E.D. della Corte di Cassazione[10].

3. Segue: il settore civile

In questa cornice generale, in conformità delle disposizioni contenute nel decreto n. 178 del 2006, occorre distinguere i provvedimenti giurisdizionali della Suprema Corte a seconda che siano adottati da sezione civili o sezioni penali[11].

---

[7] *Ibid.*

[8] *Ibid.*

[9] *Ibid.*

[10] Per la ricognizione del ruolo ordinamentale e delle funzioni assegnate agli organi della Corte di Cassazione richiamati nel testo si rinvia alle Tabelle di organizzazione della Corte di Cassazione per il triennio 2017-2019, attualmente vigenti.

[11] Tali disposizioni sono contenute nelle pagine 2 e 3 del provvedimento in esame e devono essere integrate dalle indicazioni contenute nell'allegato A dello stesso provvedimento relativo ai procedimenti che devono essere segnalati dalle cancellerie delle sezioni civili della Corte di Cassazione.

Prendendo, allora, le mosse dai provvedimenti giurisdizionali adottati dalle sezioni civili della Corte di Cassazione, deve evidenziarsi che la Cancelleria centrale civile provvede d'ufficio a segnalare i procedimenti per i quali è stata presentata una richiesta di oscuramento dei dati personali e i procedimenti per i quali l'oscuramento è obbligatorio. L'oscuramento obbligatorio, in particolare, è previsto per i procedimenti civili riguardanti le materia dell'adozione; dell'assistenza ai minori; della capacità della persona fisica; della delibazione di sentenze straniere; della famiglia; dell'interruzione di gravidanza; della responsabilità civile; del lavoro privato; dello stato civile[12].

In queste ipotesi la Cancelleria centrale civile provvede alla segnalazione dell'oscuramento, mediante «l'apposizione di una stampigliatura sul fascicolo, utilizzando i marcatori predisposti in via automatica»[13].

La medesima annotazione fascicolare, relativa all'oscuramento dei dati personali dei soggetti processuali, deve essere apposta dalle Cancellerie della Sesta Sezione civile sul fascicoletto di spoglio e delle Sezioni unite civili; ipotesi, quest'ultima, statisticamente marginale.

Un ruolo fondamentale, quindi, viene svolto dai magistrati addetti all'esame preliminare dei ricorsi, afferenti al settore civile, che devono verificare preliminarmente se i procedimenti «per i quali sussistono o possono sussistere i presupposti per disporre l'oscuramento di dati personali o identificativi risultino segnalati con le modalità sopra indicate sul relativo fascicolo […]»[14] e, in caso negativo, devono provvedere «a far apporre sul fascicolo e a fare inserire nel registro generale la relativa annotazione»[15].

Analoga verifica deve essere svolta dalle cancellerie dei singoli sezioni civili, che devono provvedere con le stesse modalità prescritte per i magistrati addetti all'esame preliminare dei ricorsi, qualora ricevano una richiesta di oscuramento dei dati personali da parte di un soggetto interessato.

Superata questa fase preliminare e assegnato il fascicolo a un'udienza civile, i singoli collegi, nei casi in cui si debba disporre l'oscuramento dei dati personali di un soggetto processuale, ai sensi dell'art. 52, commi 2 e 5, del d.lgs. n. 196 del 2003[16] ovvero in eventuale accoglimento della richiesta dell'interessato, devono fare apporre sul ruolo di udienza «un'annotazione con la quale si segnala che

---

[12] Si tratta, in particolare, dei provvedimenti giurisdizionali compiutamente elencati nell'allegato A del decreto presidenziale in esame.

[13] Si veda decreto del Primo Presidente della Corte di Cassazione 14 dicembre 2006, cit.

[14] *Ibid*.

[15] *Ibid*.

[16] *Ibid*.

prima dell'inserimento del provvedimento nella rete Internet […] debbono essere oscurati i dati in questione […]»[17].

Dopo la decisione del procedimento, l'estensore del provvedimento giurisdizionale civile, in sede di redazione della motivazione, deve indicare alla cancelleria i dati identificativi oggetto di oscuramento, avendo cura di sottolineare «con una linea continua le parole e le indicazioni numeriche non ostensibili direttamente in sede di redazione dello stesso»[18].

Depositato il provvedimento, l'Ufficio del Massimario e del Ruolo della Corte di Cassazione, in relazione alle pronunzie giudiziarie sottoposte a scrutinio ai fini della massimazione o dell'inserimento nel "Servizio Novità", deve segnalare i casi in cui si deve disporre l'oscuramento obbligatorio dei dati identificativi *ex* art. 52, comma 5, del d.lgs. n. 196 del 2003, laddove «non già indicati nel provvedimento, apponendo una barra sulle parole e sulle indicazioni non ostensibili»[19].

Infine, a completamento della descritta procedura, l'Ufficio del C.E.D. della Corte di Cassazione deve eseguire le operazioni di oscuramento dei dati identificativi dei soggetti processuali, nel rispetto delle indicazioni ricevute.

4. Segue: il settore penale

Occorre, quindi, passare a considerare le disposizioni contenute nel decreto del Primo Presidente n. 178 n. del 2006, relative alla tutela dei dati personali nei provvedimenti giurisdizionali della Suprema Corte riguardanti il settore penale[20].

Anche, in questo caso, assume un ruolo decisivo e preliminare la Cancelleria centrale penale, che provvede a segnalare «i procedimenti per i quali vi è richiesta di oscuramento dei dati personali, nonché dei procedimenti che abbiano ad oggetto reati contro la famiglia (artt. da 556 a 574-*bis* cod. pen.), reati di cui agli artt. 414-*bis* e 416, settimo comma, cod. pen., reati di cui all'artt. 591 cod. pen., reati di cui agli artt. da 600-*bis* a 600-*octies* e da 609-*bis* a 609-*undecies* cod. pen., reati di cui all'art. 643 cod. pen., reati in tema di prostituzione, reati in materia di interruzione volontaria della gravidanza, reati in materia di procreazione medicalmente assistita, reati cui all'art. 734-*bis* cod. pen., reati commessi da o in

[17] *Ibid.*

[18] *Ibid.*

[19] *Ibid.*

[20] Tali disposizioni sono contenute nelle pagine 3 e 4 del decreto in esame e devono essere integrate dalle indicazioni contenute nell'allegato B dello stesso provvedimento.

danno di minorenni […]»[21]. In tali ipotesi, la Cancelleria centrale penale procede «mediante apposizione di stampigliatura sul fascicolo, utilizzando i marcatori predisposti in via automatica»[22].

In questi casi, i magistrati addetti all'esame preliminare dei ricorsi per cassazione, afferenti al settore penale, devono verificare se i procedimenti riguardanti le materie oggetto di oscuramento e comunque quelli per i quali sussistono o possono sussistere i presupposti per disporre l'oscuramento di dati personali o identificativi, risultino «segnalati con le modalità sopra indicate sul relativo fascicolo […]»[23] e, in caso negativo, provvedono a fare «apporre sul fascicolo e a fare inserire nel registro generale la relativa annotUnazione»[24].

Analoga incombenza grava sulle cancellerie delle singole sezioni penali, che devono provvedere, con le modalità richiamate, qualora ricevano una richiesta di oscuramento dei dati personali da parte di un soggetto interessato.

Superata questa fase preliminare e assegnato il fascicolo a un'udienza penale, i singoli collegi, nei casi in cui si debba disporre l'oscuramento dei dati personali o comunque identificativi, ai sensi dell'art. 52, commi 2 e 5, del d.lgs. n. 196 del 2003, ovvero in accoglimento della richiesta dell'interessato, provvedono ad apporre sul ruolo di udienza «un'annotazione con la quale si segnala che, prima dell'inserimento del provvedimento nella rete Internet […] debbono essere oscurati i dati in questione […]»[25].

Dopo la decisione, l'estensore del provvedimento giurisdizionale penale, in sede di redazione della motivazione, provvede a segnalare i dati da oscurare, sottolineando «con una linea continua le parole e le indicazioni numeriche non ostensibili direttamente in sede di redazione dello stesso»[26].

Depositato il provvedimento, l'Ufficio del Massimario e del Ruolo della Corte di Cassazione, in relazione ai provvedimenti giurisdizionali penali sottoposti al suo scrutinio, ai fini della massimazione o dell'inserimento nel "Servizio Novità", deve segnalare i casi in cui si debba disporre l'oscuramento dei dati identificativi d'ufficio, ai sensi dell'art. 52, comma 5, del d.lgs. n. 196 del 2003, laddove non indicati nell'atto processuale, apponendo «una barra sulle parole e le indicazioni numeriche non ostensibili»[27].

---

[21] Si veda decreto del Primo Presidente della Corte di Cassazione 14 dicembre 2006, cit.; si tratta, in particolare, dei provvedimenti giurisdizionali compiutamente elencati nell'allegato B del decreto presidenziale in esame.

[22] *Ibid*.

[23] *Ibid*.

[24] *Ibid*.

[25] *Ibid*.

[26] *Ibid*.

[27] *Ibid*.

Infine, a completamento della procedura che si è richiamata, l'Ufficio del C.E.D. della Corte di Cassazione provvede ad eseguire le operazioni di oscuramento, nel rispetto delle indicazioni ricevute.

5. Gli interventi della Corte Costituzionale e la protezione dei dati personali nei provvedimenti giurisdizionali

Nella parte conclusiva di questa esposizione ci si vuole concentrare sugli interventi della Corte Costituzionale maggiormente rappresentativi delle esigenze di tutela dei dati personali che si sono esposte nei paragrafi precedenti[28].

In questa cornice, innanzitutto, occorre evidenziare che la Corte Costituzionale, a partire dalla sentenza 26 marzo 1990, n. 139[29], ha sempre ricondotto il tema della protezione dei dati personali nell'ambito del principio di tutela della riservatezza individuale, così come prefigurato dall'art. 15 Cost.

In particolare, con la sentenza n. 139 del 1990, riguardante la legittimità del d.lgs. 6 settembre 1989 n. 322, recante «Norme sul sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'art. 24 l. 23 agosto 1988 n. 440», la Corte Costituzionale evidenziava che le finalità perseguite dal principio di tutela della riservatezza individuale mirano a «prevenire qualsiasi rischio che i dati raccolti siano conosciuti all'esterno nel loro riferimento nominativo o individuale ovvero in modo tale che siffatto riferimento possa esser ricostruito pur in presenza di dati anonimi […]»[30].

La Corte Costituzionale, al contempo, evidenziava che lo scopo di «tale principio è duplice, in quanto, senza siffatte garanzie, da un lato, le statistiche potrebbero risultare non veridiche e, dall'altro lato, potrebbero essere messi in pericolo beni individuali strettamente connessi al godimento di libertà costituzionali e, addirittura, di diritti inviolabili […]»[31].

Nella stessa direzione ermeneutica si pone la sentenza 23 giugno 2005, n. 271[32], intervenuta a distanza di un quindicennio, che si pronunciava sul d.lgs. n. 196 del 2003, affermandone la legittimità, evidenziando che con tale disciplina il legislatore mirava a tutelare il trattamento dei dati personali, introducendo una disciplina – conforme al dettato costituzionale – che, pur riconoscendo tutele differenziate in relazione ai diversi tipi di dati personali e all'eterogeneità dei

[28] Si tratta, naturalmente, di un'esposizione che non ha alcuna pretesa di esaustività, mirando soltanto a fornire alcune indicazioni ermeneutiche utili a inquadrare il tema in esame.

[29] Si veda Corte cost., 26 marzo 1990, n. 139.

[30] Si veda Corte cost., 26 marzo 1990, cit.

[31] Si veda Corte cost., 26 marzo 1990, cit.

[32] Si veda Corte cost., 23 giugno 2005, n. 271.

contesti normativi in cui tali dati vengono utilizzati, si caratterizzava per il riconoscimento di una serie di diritti intangibili delle persone fisiche e giuridiche.

Il terzo e fondamentale arresto della Corte Costituzionale, al quale occorre riferirsi, è quello relativo alla sentenza 21 febbraio 2019, n. 20[33].

Con tale pronuncia la Corte Costituzionale, nel dichiarare incostituzionale l'obbligo di pubblicare *on-line* i dati personali sul reddito e sul patrimonio dei dirigenti pubblici diversi da quelli che ricoprono incarichi apicali, tratteggiava in maniera efficace e aderente all'attuale stato del pensiero giuridico il fondamento costituzionale del diritto alla riservatezza dei dati personali, che costituisce un risvolto della manifestazione del diritto fondamentale all'intangibilità della sfera privata[34].

Secondo il Giudice costituzionale, nell'epoca attuale, il diritto alla riservatezza si atteggia principalmente quale diritto a controllare la circolazione delle informazioni riferite alla persona, che si giova, a sua protezione, dei canoni elaborati in sede sovranazionale per valutare la legittimità della raccolta, del trattamento e della diffusione dei dati personali[35].

La Corte Costituzionale, inoltre, tenuto conto dell'affermazione degli strumenti digitali e del progresso tecnologico, che permettono una rapida e indiscriminata diffusione delle informazioni tramite la rete e le comunicazioni telematiche, prefigurava una "nozione dinamica" del diritto alla riservatezza, idonea a consentire all'interessato di controllare la diffusione dei suoi dati e di reagire di fronte a comportamenti illegittimi dei soggetti che intervengono nelle operazioni di trattamento dei dati personali[36].

Naturalmente, il diritto alla riservatezza può subire deroghe o limitazioni, che, tuttavia, si devono ispirare ai principi di proporzionalità, pertinenza e non eccedenza nel trattamento dei dati personali, in modo da operare nei limiti indispensabili a consentire di raggiungere obiettivi legittimi, sottesi all'acquisizione e alla diffusione delle informazioni. Diventa, pertanto, indispensabile identificare le misure che incidono in modo limitato sul diritto alla riservatezza dell'individuo, contribuendo al contempo al raggiungimento di legittimi obiettivi informativi.

D'altra parte, secondo la Corte Costituzionale, eguale rilievo deve essere riconosciuto ai principi di pubblicità e di trasparenza, rilevanti, non solo, quali corollari del principio democratico di cui all'art. 1 Cost. per tutti gli aspetti rilevanti della vita pubblica, ma, anche, ai sensi dell'art. 97 Cost., per il buon funzionamento della pubblica amministrazione e per la gestione dei dati che la stessa possiede e controlla.

---

[33] Si veda Corte cost., 21 febbraio 2019, n. 20.

[34] Si veda Corte cost., 21 febbraio 2019, cit.

[35] Si veda Corte cost., 21 febbraio 2019, cit.

[36] Si veda Corte cost., 21 febbraio 2019, cit.

Celestina Iannone e Emma Salemme[1]

L'anonimizzazione delle decisioni giudiziarie della Corte di Giustizia e dei giudici degli Stati membri dell'Unione europea

1. Introduzione

La pubblicazione delle sentenze ha costituito nel tempo un fattore di salvaguardia dell'accesso libero e completo alla giurisprudenza ed in particolare alla motivazione delle decisioni di giustizia. Attualmente, tuttavia, la diffusione del contenuto di tali decisioni attraverso i mezzi di comunicazione telematici pone una serie di problematiche nuove, relative in particolare alla protezione dei dati personali dei soggetti coinvolti.

---

[1] Celestina Iannone è direttrice della Direzione della Ricerca e Documentazione della Corte di Giustizia dell'Unione europea. Emma Salemme è amministratrice nella medesima Direzione. Le opinioni espresse nel presente contributo sono frutto esclusivo del pensiero delle autrici e non impegnano in alcuno modo l'istituzione di appartenenza.

In effetti, con l'evoluzione delle tecnologie informatiche e dei mezzi di comunicazione telematici che consentono una sempre più rapida circolazione di dati e informazioni, il diritto alla riservatezza dei soggetti cui le informazioni ineriscono è sottoposto a nuove e potenziali minacce e, come tale, esige la creazione di garanzie sempre più stringenti. Al giorno d'oggi è infatti possibile, partendo dal nome di una persona fisica, entrare in possesso di una moltitudine di informazioni riguardanti diversi aspetti della sua vita privata, incluso il profilo giudiziario, con tutte le conseguenze pregiudizievoli che ne derivano.

Le normative internazionali offrono la base per l'elaborazione di norme che permettono di trovare un equilibrio tra l'esigenza di accesso alla giustizia e la protezione dei dati personali.

L'articolo 6 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) coniuga infatti il principio della trasparenza dei provvedimenti giudiziari con la tutela della riservatezza disponendo, da un lato, che ogni persona ha diritto a che le sentenze siano rese pubblicamente, dall'altro, che il principio di pubblicità possa essere limitato quando lo esigono gli interessi dei minori, la protezione della vita privata delle parti in causa, il rischio di pregiudizio agli interessi della giustizia, all'ordine pubblico o alla sicurezza nazionale.

Tali principi si ritrovano consacrati altresì nell'articolo 47, comma 2, della Carta dei diritti fondamentali dell'Unione europea, la quale prevede il diritto di ogni persona a che la sua causa sia esaminata pubblicamente, e negli articoli 7 e 8 che consacrano il diritto alla protezione della vita privata e alla protezione dei dati personali.

D'altro canto, in entrambi gli strumenti internazionali, il diritto al rispetto della vita privata e alla protezione dei dati personali non sono dei diritti assoluti e devono, pertanto, conciliarsi con gli altri principi fondamentali, quali appunto il citato principio di pubblicità delle sentenze e la libertà fondamentale d'informazione ed espressione, garantiti dall'articolo 10 della CEDU e dell'articolo 11 della Carta dei diritti fondamentali[2].

L'entrata in vigore del regolamento UE 2016/679, noto come GDPR (General Data Protection Regulation)[3], nonché della direttiva (UE) 2016/680[4] che regola i

---

[2] S. Van Raepenbusch, *Anonymisation des décisions de la Cour justice de l'Union européenne, protection de la vie privée versus publicité des jugements*, in *Chronique de jurisprudence*, 1er août 2000 – 31 décembre 2001, 341 et 342, e J. Mont, *RGDP: faut-il anonymiser la jurisprudence publiée ?,* in *Journal des Tribunaux*, 2019, (6776), 444, http://www.crid.be/pdf/public/8448.pdf.

[3] 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) (GU L 119, 4.5.2016, p. 1-88).

[4] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla

trattamenti di dati personali nelle attività di prevenzione, contrasto e repressione dei crimini[5], ha innalzato i livelli di protezione dei dati personali e responsabilizzato i soggetti preposti al trattamento degli stessi. Il GDPR, la cui base giuridica si ritrova nell'articolo 16 del TFUE, intende infatti garantire e bilanciare la protezione dei dati di carattere personale con l'esigenza di assicurare il pieno esercizio della libera circolazione. Tale regolamento ha come scopo principale di rinforzare la protezione dei dati personali, in particolare di quelli "sensibili" (riguardanti l'origine razziale e etnica, le opinioni politiche, le convinzioni religiose e filosofiche, l'appartenenza sindacale, ed anche i dati genetici, biometrici, intesi ad identificare in modo univoco una persona fisica, nonché i dati relativi alla salute, alla vita sessuale e all'orientamento sessuale) dando la possibilità al cittadino di controllarne la divulgazione e di esercitare il diritto all'oblio.[6] La direttiva (UE) 2016/680, che costituisce una *lex specialis* rispetto al GDPR, introduce poi norme specifiche sulla protezione delle persone fisiche nelle procedure di prevenzione, indagine, accertamento e perseguimento dei reati nonché nell'esecuzione delle sanzioni penali. Sia il GDPR che la direttiva si applicano alle attività degli organi giudiziari.

Tuttavia, in relazione a tale attività, il regolamento prevede alcune eccezioni, consentendo l'introduzione di una normativa specifica a livello nazionale. Il considerando numero 20, infatti, stabilisce che "il diritto dell'Unione o degli Stati membri potrebbe specificare le operazioni e le procedure di trattamento relativamente al trattamento dei dati personali effettuato da autorità giurisdizionali e da altre autorità giudiziarie". Al fine di salvaguardare l'indipendenza della magistratura nell'adempimento delle competenze giurisdizionali, l'autorità preposta al controllo del trattamento dei dati personali da parte delle autorità giurisdizionali non è quindi tenuta ad estendere il suo controllo alle funzioni giurisdizionali. Inoltre, i dati "sensibili" possono essere oggetto di trattamento allorquando questo "è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali" (art. 9, par. 2, lett. F). Alla luce del principio della salva-

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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89-131).

[5] Tale direttiva è stata attuata nell'ordinamento giuridico italiano attraverso il d.lgs. 18 maggio 2018, n. 51.

[6] J.C. Wiwinius, *La diffusion de la jurisprudence au regard de la protection des données personnelles*, in *Colloque de l'AHJUCAF*, Beyrouth (Liban), 13-14 juin 2019, *La diffusion de la jurisprudence des Cours suprêmes judiciaires francophones au temps d'internet*.

guardia dell'autonomia della magistratura, il GDPR non impone dunque l'anonimizzazione delle decisioni di giustizia.

Inoltre, tale regolamento si applica solo all'interno degli ordinamenti nazionali e non riguarda le attività delle istituzioni europee e dunque l'attività giudiziaria della Corte di Giustizia dell'Unione europea.

Alle istituzioni europee e alla Corte si applica il regolamento (UE) 2018/1725[7]. Quest'ultimo contiene e si ispira agli stessi principi di "necessità di bilanciamento" tra l'esigenza di garantire l'accesso all'informazione e la protezione dei dati personali e introduce altresì la regola generale della "responsabilità del titolare del trattamento". In particolare, l'articolo 5 (a) del regolamento 2018/1725 sancisce che il trattamento dei dati personali è lecito quando esso "è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri di cui sono investiti l'istituzione o l'organo dell'Unione". Il regolamento si applica dunque al trattamento dei dati personali nell'attività di amministrazione della giustizia della Corte. Tuttavia prevede, come il GDPR, la limitazione dell'applicazione della stessa disciplina nell'ambito dell'attività giudiziaria [(art. 25, paragrafo 1, lett. e)]. Pertanto, il delegato alla protezione dei dati personali della Corte di Giustizia è responsabile del trattamento dei dati contenuti in documenti "non strettamente collegati" all'attività giudiziaria. Inoltre, anche tale regolamento non impone l'anonimizzazione delle decisioni giudiziarie.

Tuttavia, sebbene il GDPR e il regolamento 2018/1725 non impongano tale anonimizzazione, dei procedimenti di anonimizzazione delle sentenze sono stati introdotti sia alla Corte di Giustizia dell'Unione europea sia in vari ordinamenti nazionali.

2. L'anonimizzazione delle decisioni della Corte di Giustizia

Prima di entrare nel merito delle regole applicabili all'anonimizzazione delle sentenze della Corte di Giustizia, è importante fare un accenno alla modalità di pubblicazione degli atti di procedura.

Di tutte le domande di decisione pregiudiziale e di tutti i ricorsi diretti promossi davanti ai due organi giudiziari, è data comunicazione sulla Gazzetta Ufficiale dell'Unione europea (G.U.U.E.), in tutte le lingue ufficiali dell'Unione. Inoltre, a partire dal 2018, le ordinanze di rinvio pregiudiziale sono accessibili sul sito della Corte, nelle versioni linguistiche disponibili.

---

[7] 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 (OJ L 295, 21.11.2018, p. 39-98).

Tutte le pronunce dei due organi giudiziari sono pubblicate nella Raccolta della giurisprudenza, accessibile online. Delle stesse è diffusa una comunicazione sulla G.U.U.E.. Inoltre le pronunce sono accessibili in extenso sul sito web della Corte (CURIA) e sul sito della Commissione (Eur-Lex). Tali siti offrono dei formulari di ricerca anche avanzata, i quali permettono di individuare e ripercorrere la giurisprudenza su una determinata questione di diritto ma anche su una determinata persona fisica e giuridica. Le sentenze principali sono accessibili in tutte le lingue ufficiali, le altre sono pubblicate in francese e nella lingua di procedura. L'accesso è dunque totale.

Le regole di procedura, inoltre, non impongono l'anonimizzazione in nessuna delle procedure del contenzioso dell'Unione. Ai sensi dell'art. 95 del Regolamento di procedura della Corte:

"1. Quando l'anonimato è stato concesso dal giudice del rinvio, la Corte rispetta detto anonimato nell'ambito del procedimento dinanzi ad essa pendente.
2. Su domanda del giudice del rinvio, su domanda debitamente motivata di una parte nel procedimento principale o d'ufficio, la Corte, qualora lo reputi necessario, può inoltre procedere a coprire con l'anonimato una o più persone o enti interessati dalla controversia."

Il Regolamento di procedura prevede dunque tre tipologie di circostanze che possano giustificare l'oscuramento dei dati personali: (1) il giudice nazionale ha già concesso l'anonimato nella causa principale, (2) sia stata inoltrata una richiesta dal giudice del rinvio oppure da una o più persone coinvolte nella procedura e (3) la Corte dispone l'anonimizzazione d'ufficio.

2.1. L'anonimizzazione nella procedura pregiudiziale

A partire dal primo luglio 2018, la Corte ha deciso di rafforzare la protezione dei dati delle persone fisiche nell'ambito delle pubblicazioni relative alle cause pregiudiziali. In questa sezione verrà illustrata la nuova disciplina sull'anonimizzazione applicabile alle cause pregiudiziali a partire da luglio 2018 (2.1.2.) nonchè le regole applicabili alle procedure pregiudiziali non anonimizzate (2.1.3.).

2.1.2. Il nuovo orientamento inaugurato nel luglio del 2018

Nel luglio del 2018, in seguito all'adozione del GDPR e prima dell'entrata in vigore del regolamento 2018/1725, la Corte ha ritenuto opportuno modificare la sua disciplina in materia di protezione dei dati delle persone fisiche nell'ambito delle pubblicazioni relative alle cause pregiudiziali. Se sino a quella data, la pubblicità dei nomi negli atti di causa e nelle pronunce era la regola, l'anonimizzazione l'eccezione (ai sensi dell'art. 95 del Regolamento di procedura della Corte),

a partire da quella data questo rapporto tra regola ed eccezione è stato invertito, al fine garantire il livello di tutela dei dati personali imposto dal GDPR.

Nel concepire la nuova disciplina, la Corte ha cercato di trovare un giusto equilibrio tra il diritto di accesso alla giustizia ed i diritti fondamentali sanciti dagli articoli 7 e 8 della Carta. Tale equilibrio deve prendere in considerazione, da un lato, la natura delle informazioni ricercate e l'impatto sulla vita privata dei soggetti coinvolti in caso di diffusione delle stesse e, dall'altro, l'interesse del pubblico ad avere accesso a tali informazioni, considerando tuttavia che tale interesse può variare a seconda del ruolo che la persona in questione ha nella vita pubblica[8]. Proprio in considerazione di queste opposte esigenze ed in considerazione della propria giurisprudenza in materia di protezione dei dati personali, la Corte ha deciso di offrire un maggiore accesso agli atti di procedura, con la diffusione delle ordinanze di rinvio, ed allo stesso tempo ha fissato delle regole più stringenti di protezione dei dati personali.

Nella decisione diffusa con il comunicato stampa n. 96/18 del 29 giugno 2018[9], si legge che "per assicurare la protezione dei dati delle persone fisiche coinvolte nelle cause pregiudiziali, garantendo nel contempo l'informazione dei cittadini e la pubblicità della giustizia, la Corte di giustizia ha […] deciso, per ogni causa pregiudiziale presentata a partire dal 1° luglio 2018, di sostituire con iniziali, in tutti i documenti pubblicati, i nomi delle persone fisiche coinvolte nella causa. Allo stesso modo, sarà eliminato qualsiasi elemento supplementare atto a consentire l'identificazione delle persone implicate".

È inoltre indicato che la nuova pratica si applica "a tutte le pubblicazioni che possono aver luogo nell'ambito della trattazione della causa, dalla sua presentazione fino alla sua conclusione (comunicazioni nella Gazzetta Ufficiale, conclusioni, sentenze...), e altresì alla denominazione della causa".

Inoltre, nelle raccomandazioni ai giudici nazionali relative all'introduzione di domande pregiudiziali[10], le quali contengono indicazioni sulla forma e sul contenuto della domanda di pronuncia pregiudiziale, il punto 21 invita i giudici di rinvio a rendere anonime le loro domande di pronuncia pregiudiziale:

---

[8] S. Van Raepenbusch, *Anonymisation des décisions de la Cour justice de l'Union européenne, protection de la vie privée versus publicité des jugements*, in *Chronique de jurisprudence*, 1er août 2000 – 31 décembre 2001, 339.

[9] Comunicato stampa della Corte di Giustizia UE n. 96/18, del 29 giugno 2018, https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180096it.pdf

[10] Raccomandazioni all'attenzione dei giudici nazionali, relative alla presentazione di domande di pronuncia pregiudiziale (2019/C 380/01), disponibile al: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:JOC_2019_380_R_0001

"Per garantire la protezione ottimale dei dati personali nell'ambito della trattazione della causa da parte della Corte, della notifica della domanda di pronuncia pregiudiziale agli interessati di cui all'articolo 23 dello Statuto[11] e della ulteriore diffusione, in tutte le lingue ufficiali dell'Unione, della decisione che conclude il giudizio, il giudice del rinvio, che è il solo a disporre di una conoscenza integrale del fascicolo trasmesso alla Corte, è invitato a effettuare l'anonimizzazione della causa sostituendo, ad esempio attraverso iniziali o una combinazione di lettere, il nome delle persone fisiche menzionate nella domanda e omettendo gli elementi che potrebbero consentire di identificare tali persone. A causa dell'uso crescente delle nuove tecnologie dell'informazione e, segnatamente, del ricorso ai motori di ricerca, un'anonimizzazione effettuata dopo la notifica della domanda di pronuncia pregiudiziale agli interessati di cui all'articolo 23 dello Statuto e la pubblicazione nella Gazzetta ufficiale dell'Unione europea della comunicazione relativa alla causa considerata può infatti rivelarsi meno efficace."

Al punto 24 di tali raccomandazioni, si precisa che la domanda di pronuncia pregiudiziale deve essere accompagnata da tutti i documenti pertinenti e utili per la trattazione della causa da parte della Corte e, in particolare, da precisi recapiti delle parti in causa e degli eventuali rappresentanti di tali parti.

Quindi, da un lato, le raccomandazioni invitano i giudici nazionali ad anonimizzare le loro ordinanze di rinvio pregiudiziale, dall'altro, chiedono di comunicare, con atto separato, i dati relativi alle parti in causa.

Infine, il punto 7 delle istruzioni pratiche alle parti in merito alle cause promosse dinanzi alla Corte[12] dispone che tutti gli interessati di cui all'articolo 23 dello Statuto sono invitati, nelle loro osservazioni scritte o orali, a rispettare l'anonimato concesso alle cause pregiudiziali, indipendentemente dal fatto che tale anonimizzazione sia stata effettuata dalla Corte o dal giudice del rinvio.

In vista di tale riforma, si è riflettuto sulla possibilità di estendere l'anonimizzazione anche ai nomi dei giudici, al fine di evitare il rischio della elaborazione di algoritmi informatici che permettano di creare, con dei dati di "giustizia predittiva", i presupposti per un "forum shopping". La Corte non ha per il momento

---

[11] Secondo l'articolo 23, primo comma, dello Statuto della Corte: "Nei casi contemplati dall'articolo 267 del trattato sul funzionamento dell'Unione europea la decisione del giudice nazionale che sospende la procedura e si rivolge alla Corte di giustizia è notificata a quest'ultima a cura di tale giudice nazionale. Tale decisione è quindi notificata a cura del cancelliere della Corte alle parti in causa, agli Stati membri e alla Commissione, nonché all'istituzione, all'organo o all'organismo dell'Unione che ha adottato l'atto di cui si contesta la validità o l'interpretazione." (disponibile al link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A12008E%2FPRO%2F03)

[12] Istruzioni pratiche alle parti, relative alle cause proposte dinanzi alla Corte, disponibili al: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.LI.2020.042.01.0001.01.ITA&toc=OJ:L:2020:042I:TOC

ritenuto necessario di procedere all'oscuramento dei nomi dei componenti della formazione giudicante, considerando tale dato ancora essenziale per il regime di pubblicità delle sentenze.

2.1.3. Il trattamento delle domande di decisione pregiudiziale non rese anonime dal giudice nazionale

In questa sezione saranno presentate le modalità con cui sono trattate le cause non anonimizzate dalla giurisdizione di rinvio. Più precisamente, verrà illustrato il modo in cui tali cause sono designate (2.1.3.1.) nonché la procedura di anonimizzazione interna alla Corte (2.1.3.2.).

2.1.3.1. Le modalità di designazione delle cause e delle sentenze

Il procedimento di anonimizzazione consiste nell'oscurare, nel corpo del rinvio pregiudiziale e successivamente in tutti gli atti della causa sino alla pronuncia finale, il cognome e il nome delle persone fisiche menzionate. Il nome è sostituito con una sigla (diversa dalle iniziali). I dati delle persone giuridiche sono invece resi anonimi solo in casi eccezionali, d'ufficio o su richiesta debitamente motivata. Tale procedimento può altresì comportare la cancellazione di qualsiasi informazione supplementare che possa consentire di identificare tali persone.

Inoltre, quando una causa pregiudiziale è resa anonima dalla Corte, la cancelleria propone altresì che le venga attribuito un nome d'uso, secondo le seguenti linee:

– se tra le parti in causa vi sono una o più persone fisiche e una o più persone giuridiche (che possono essere, in particolare, autorità pubbliche o enti pubblici), la denominazione usuale della causa corrisponderà a quella di una delle persone giuridiche ricorrenti nella causa principale [per esempio: la causa C-188/15, Bougnaoui e ADDH – tra la sig.ra Asma Bougnaoui e l'Association de défense des droits de l'homme (ADDH) e la società Micropole – avrebbe il seguente nome d'uso: Causa C-188/15, ADDH].
– se la causa contrappone una o più persone fisiche a una o più persone giuridiche (in particolare, autorità pubbliche o enti pubblici), il nome d'uso della causa deve corrispondere a quella di una delle persone giuridiche, convenuta nella causa principale (per esempio: la causa C-528/13, Léger – tra Geoffrey Léger e il ministro degli Affari sociali, della sanità e dei diritti della donna e l'Istituto francese del sangue – avrebbe il seguente nome d'uso: Causa C-528/13, Istituto francese del sangue);
– se la causa è intentata esclusivamente da persone fisiche, il nome d'uso della causa corrisponde alla sigla attribuita dalla cancelleria al ricorrente nella

causa principale o al primo delle parti (per esempio: la causa C-497/10 PPU, Mercredi – tra Barbara Mercredi e Richard Chaffe – avrebbe il seguente nome d'uso: Causa C-497/10 PPU, AZ).

Il giudice relatore e l'avvocato generale, se ritengono che il nome d'uso della causa non sia sufficientemente distintivo, possono proporre di attribuire alla causa un nome "convenzionale", destinato a comparire, tra parentesi, dopo il nome d'uso della causa. Ciò può accadere quando la causa è intentata esclusivamente da persone fisiche e il nome d'uso della causa anonimizzata è quindi costituito dalle iniziali attribuite al ricorrente o quando una causa precedente ha lo stesso nome d'uso (per esempio quello di una persona giuridica che è parte in più cause dinanzi alla Corte di Giustizia).

Il nome convenzionale può essere stabilito, in particolare, sulla base del nome di una persona giuridica che non ha la qualità di parte nella causa principale, ma che è nominata nell'ordinanza di rinvio e interessata dalla causa, oppure sulla base dell'oggetto o delle questioni sollevate nella controversia. In tal caso, il nome della causa è seguito, tra parentesi, dal nome convenzionale [per esempio, C-528/13, XY (Donazione di sangue)].

La decisione in merito a queste proposte è adottata durante la riunione generale della Corte sulla base della proposta presentata dal giudice relatore e dall'avvocato generale e, per le procedure pregiudiziali di urgenza, nella riunione amministrativa della sezione che si occupa di tali procedure.

2.1.3.2. La procedura di anonimizzazione

La procedura di anonimizzazione interna alla Corte è attivata solo nel caso in cui il giudice del rinvio non abbia adottato misure atte a garantire la protezione dei dati personali nel testo dell'ordinanza di rinvio. La cancelleria della Corte è responsabile di tale procedura, che si compone di molteplici tappe.

Preparazione della versione anonima della domanda di pronuncia pregiudiziale da parte della cancelleria

Quando una domanda di decisione pregiudiziale contiene informazioni relative al nome o all'identità di una o più persone fisiche – siano esse parti della causa principale o persone fisiche terze menzionate nella domanda – la cancelleria inserisce la versione originale, detta "nominativa" nel fascicolo elettronico della causa, cui hanno accesso unicamente i membri della Corte.

In parallelo, la cancelleria redige una versione "anonima", con l'assistenza di un giurista-linguista dell'unità della lingua di procedura della Direzione generale del multilinguismo e di un giurista dello Stato di appartenenza del giudice di rinvio della Direzione Ricerca e Documentazione.

La versione anonima dell'ordinanza di rinvio è inserita nel fascicolo originale della causa, il quale è accessibile, in cancelleria, a tutti gli interessati di cui all'articolo 23 dello Statuto, aventi il diritto di presentare osservazioni scritte e orali.

Il cancelliere redige una tabella di corrispondenza che riporta i cognomi e i nomi effettivi delle persone interessate e le sigle loro assegnate e, se del caso, le eventuali informazioni supplementari che sono state cancellate. Tale tabella è notificata, insieme all'ordinanza di rinvio, alle parti in causa e al giudice nazionale ed è inserita nel fascicolo elettronico della causa accessibile solo ai membri della Corte.

Esame della versione anonima da parte della Direzione Ricerca e Documentazione e della Direzione generale del Multilinguismo

La Direzione della Ricerca e Documentazione redige una nota di analisi preliminare della domanda pregiudiziale sulla base della versione nominativa. La Direzione può anche, alla luce della versione anonima preparata dalla cancelleria e della tabella di correlazione, formulare delle proposte di modifica soprattutto ai fini della protezione dei dati personali ivi contenuti. In particolare, può proporre (1) di estendere l'anonimizzazione al di là della sostituzione dei nomi degli interessati con delle iniziali, in considerazione della particolare natura o sensibilità del caso, (2) di ristabilire l'identità delle parti interessate, ad esempio quando ciò sia giustificato dall'oggetto della controversia, dal diritto all'informazione del pubblico o dalle particolari circostanze del caso.

Inoltre, ogni domanda pregiudiziale nella versione originale (nominativa) è tradotta in francese, la lingua di lavoro della Corte. La traduzione in lingua francese è inserita nell'archivio elettronico della causa. Ai fini della traduzione in tutte le lingue, la versione utilizzata dalla Direzione generale del Multilinguismo, che include gli omissis e l'eventuale riassunto, è invece quella anonima preparata dalla cancelleria.

Esame della versione anonima da parte del giudice relatore e dell'avvocato generale

Ai fini della redazione della relazione preliminare, il giudice relatore e l'avvocato generale possono proporre che la causa sia trattata nominativamente se ritengono giustificato il ripristino dell'identità delle parti interessate, in particolare a causa delle obiezioni sollevate sull'anonimato dalle parti della causa principale o per altri motivi specifici. Essi possono anche proporre alla Corte di estendere l'esigenza di anonimizzazione ad altri dati contenuti nell'ordinanza di rinvio o, al contrario, di ridurre i dati oscurati. A tale riguardo, essi tengono conto sia del parere espresso dal cancelliere e dalla Direzione della Ricerca e Documentazione, in sede di analisi preliminare del caso, sia dell'eventuale posizione del giudice di rinvio su tale questione.

Notifica alle parti interessate e pubblicazione della domanda pregiudiziale

La versione anonima, o la sua sintesi, è notificata alle parti interessate di cui all'articolo 23 dello Statuto.

Prima di effettuare tale notifica, la cancelleria comunica alle parti della causa principale la tabella di corrispondenza da essa predisposta, invitandole a presentare le loro eventuali osservazioni sull'anonimizzazione effettuata dalla Corte. A meno che non si oppongano a tale anonimizzazione, le parti sono pregate di non menzionare nelle loro osservazioni scritte alcun nome o informazione aggiuntiva che possa consentire di identificare nuovamente gli interessati.

La versione anonima della domanda è pubblicata sul sito web della Corte dieci giorni dopo la notifica.

Avviso sulla Gazzetta Ufficiale relativa all'introduzione del caso e creazione dei metadati

L'avviso relativo all'introduzione della causa, pubblicata sulla Gazzetta Ufficiale dell'Unione europea, è redatto sulla base delle sigle assegnate dalla cancelleria. I nomi effettivi delle parti della causa principale non compaiono né nel titolo dell'avviso né nella sezione dell'avviso che menziona i nomi delle parti in causa.

Le sigle assegnate dalla cancelleria sostituiscono altresì i nomi effettivi delle parti in causa nei metadati che alimentano le banche dati, a meno che la Corte non decida che le pubblicazioni relative alla causa debbano essere nominative.

Svolgimento dell'udienza

Poiché le misure di cui sopra mirano principalmente a garantire una protezione adeguata dei dati personali nell'ambito delle pubblicazioni della Corte di Giustizia, l'udienza, che di norma è pubblica, si svolge attenendosi alle stesse regole di anonimizzazione. Pertanto, le parti e gli interessati che presentano le osservazioni si riferiscono alla causa con il suo numero di ruolo e il suo nome d'uso, eventualmente integrato dal nome convenzionale assegnatole.

Conclusioni dell'avvocato generale e decisione finale

Le conclusioni dell'avvocato generale e le sentenze sono pubblicate solo nella versione anonima che non menziona né i nomi delle persone fisiche né gli altri dati personali che sono stati eventualmente oscurati.

L'uso delle iniziali non pregiudica, ovviamente, la possibilità di inserire nel corpo del testo la qualità di parte processuale (ad esempio "il richiedente" piuttosto che "XZ") o giuridica (ad esempio "il coniuge") delle persone interessate, al fine di facilitare la leggibilità dei testi.

La versione autentica delle conclusioni e della decisione resta comunque quella nominativa che è firmata dall'avvocato generale e dal collegio giudicante e viene notificata alle parti della causa principale e al giudice del rinvio.

Avviso sulla Gazzetta Ufficiale, comunicati stampa, sintesi e massime

L'avviso della chiusura del procedimento, pubblicato nella Gazzetta Ufficiale dell'Unione europea, il comunicato stampa relativo alle conclusioni dell'avvocato generale e alla decisione, nonché l'eventuale sintesi e massimizzazione sono redatti facendo riferimento alla versione anonima della decisione e utilizzando le iniziali degli interessati nel corpo dei documenti.

Decisioni emesse dai giudizi nazionali in seguito alla pronuncia pregiudiziale

Il giudice nazionale di rinvio è invitato a trasmettere alla Corte la decisione definitiva adottata nel procedimento principale in seguito alla pronuncia pregiudiziale[13]. Tali decisioni non sono sistematicamente anonimizzate in sede nazionale e vengono registrate nelle banche dati interne alla Corte nella versione inviata dal giudice nazionale. Solo le decisioni nazionali rese anonime sono accessibili sul sito della Corte.

2.1.4. Il trattamento di una domanda di decisione pregiudiziale anonimizzata dal giudice del rinvio

Qualora la Corte di Giustizia riceva una domanda di decisione pregiudiziale in una versione già resa anonima dal giudice del rinvio (o qualora la Corte riceva due versioni della domanda, di cui una è già resa anonima), essa procederà utilizzando la sigla scelta dal giudice del rinvio (articolo 95 del Regolamento di procedura della Corte). L'aggiunta di un nome convenzionale per facilitare l'identificazione della causa rimane ovviamente possibile.

La cancelleria e la Direzione della Ricerca e Documentazione possono comunque richiedere di sottoporre tale versione anonima ad ulteriori operazioni di anonimizzazione, qualora ciò si riveli necessario per garantire un'adeguata protezione dei dati personali delle persone fisiche che sono parti del procedimento principale o dei terzi menzionati nell'ordinanza.

2.2. L'anonimizzazione nelle procedure promosse da ricorsi diretti

Per tutte le procedure introdotte davanti alla Corte con ricorsi diretti, le regole di cui all'articolo 95 del Regolamento di procedura si applicano senza alcuna

[13] Raccomandazioni all'attenzione dei giudici nazionali, relative alla presentazione di domande di pronuncia pregiudiziale (2019/C 380/01), cit., punto 32.

deroga. L'anonimato è dunque applicato solo su richiesta delle parti o di ufficio. Di fatto, per tali ricorsi, che coinvolgono principalmente le istituzioni e gli Stati, l'esigenza dell'anonimato viene riscontrata molto raramente.

L'articolo 190, paragrafo 3, del Regolamento di procedura della Corte di Giustizia prevede inoltre che l'articolo 95 si applica, *mutatis mutandis*, alle impugnazioni. Per tali procedure, la Corte si attiene dunque alla scelta del Tribunale. La Corte rispetta l'anonimato concesso dal Tribunale e le parti del procedimento sono invitate a rispettare tale trattamento anche nel procedimento dinanzi alla Corte (punto 8 delle istruzioni pratiche alle parti). Tuttavia, su domanda motivata di una parte o d'ufficio, la Corte può se lo ritiene necessario, sostituire il nome di una o più persone fisiche menzionate nell'ambito della procedura di primo grado con una sigla.

In ogni caso, quando una parte in un procedimento dinanzi alla Corte auspica che la sua identità o determinati dati che la riguardano non siano divulgati nell'ambito di una causa promossa dinanzi alla Corte o, al contrario, quando tale parte chiede che la sua identità e detti dati siano divulgati, essa ha facoltà di rivolgersi alla Corte affinché quest'ultima decida sull'anonimizzazione, totale o parziale, della causa. Per garantire l'efficacia della richiesta, è consigliato alle parti di inoltrarla il più rapidamente possibile (punto 9 delle istruzioni pratiche).

Per quanto riguarda i procedimenti dinanzi al Tribunale, l'articolo 66 del Regolamento di procedura prevede che su domanda motivata di una parte o d'ufficio, il Tribunale può omettere il nome di una parte in causa o quello di terzi menzionati nell'ambito del procedimento, oppure determinati dati nei documenti della causa cui il pubblico ha accesso, qualora ragioni legittime giustifichino che l'identità di una persona o il contenuto di tali dati siano tenuti riservati.

3. L'anonimizzazione delle decisioni dei giudici degli Stati membri dell'Unione europea

Ai fini della presentazione delle regole nazionali sull'anonimizzazione delle decisioni giudiziarie, sono qui di seguito esposte le conclusioni di uno studio di diritto comparato svolto dalla Direzione Ricerca e Documentazione della Corte di Giustizia[14]. Saranno, in primo luogo, illustrate le regole nazionali di base sulla

[14] Lo studio di diritto comparato è disponibile in inglese e in francese ai seguenti link: (fr) https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-02/ndr_2017-002_neutralisee-finale.pdf e (en) https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-02/ndr_2017-002_neutralisee-en.pdf

anonimizzazione delle decisioni giudiziarie[15] (3.1.), in secondo luogo, le modalità di tale anonimizzazione (3.2.), ed infine i regimi applicabili per la pubblicazione delle domande di pronuncia pregiudiziale (3.3.).

3.1. Le regole nazionali sull'anonimizzazione

Nei regimi nazionali analizzati, si possono identificare tre orientamenti principali: l'anonimato come principio (3.1.1.), l'anonimato come eccezione (3.1.2.), l'anonimato applicato solo nelle procedure incardinate dinanzi ad alcuni organi giudiziari (3.1.3.).

3.1.1. L'anonimato come principio

In un primo gruppo di ordinamenti giuridici vige il principio dell'anonimato per tutte le decisioni giudiziarie, a prescindere dall'organo giudicante. É il caso di ben dodici ordinamenti (diritto austriaco, bulgaro, danese, olandese, finlandese, tedesco, greco, ungherese, lussemburghese, portoghese, slovacco e svedese).

Tuttavia, nella maggior parte di questi ordinamenti, tale principio di anonimizzazione incontra dei limiti. In molti casi, l'anonimato si applica solo alle persone fisiche, sono escluse dunque le persone giuridiche (diritto bulgaro, greco, lussemburghese[16], olandese[17], slovacco e svedese) o gli enti pubblici (diritto austriaco, finlandese, ungherese e portoghese[18]). Inoltre, in cinque ordinamenti è esclusa l'anonimizzazione qualora essa possa pregiudicare la corretta comprensione della decisione, (diritto austriaco, tedesco, ungherese, olandese e slovacco). Talvolta, l'obbligo di anonimizzazione è meno stringente nelle procedure riguardanti settori specifici come il diritto dei marchi (diritto tedesco e portoghese) e il diritto della concorrenza (diritto tedesco).

3.1.2. L'anonimato come eccezione

In un secondo gruppo di ordinamenti, la regola generale è l'assenza di anonimato nella pubblicazione delle decisioni giudiziarie. L'anonimizzazione,

---

[15] Questo lavoro si concentra in particolare sulle decisioni adottate dalle Corti supreme degli Stati membri.

[16] Nel diritto lussemburghese, l'esclusione delle persone giuridiche dal campo dell'anonimizzazione sembra essere limitato alle banche.

[17] Secondo il diritto olandese, l'anonimizzazione delle persone giuridiche è praticata in determinate materie, in particolare nel diritto fiscale.

[18] Tuttavia, ciò non si applica alle decisioni del Tribunale amministrativo supremo portoghese.

che qui avviene solo in casi eccezionali, può riguardare, da un lato, tipologie di cause specificamente previste dalla legge e, dall'altro, essere disposta dal giudice competente, in presenza di condizioni che giustifichino tale trattamento.

Questa disciplina si ritrova negli ordinamenti irlandese, italiano e maltese.

Una particolare riflessione merita la normativa vigente in Irlanda, in cui l'anonimizzazione è considerata come un'eccezione al principio costituzionale dell'amministrazione pubblica della giustizia, sancito dall'articolo 34.1 della Costituzione. Tale principio implica che tutti gli atti di procedura, contenenti dati personali delle parti, siano accessibili al pubblico. Di norma, tutte le decisioni giudiziarie rese dai Tribunali irlandesi sono dunque pubblicate in internet con l'indicazione dei nomi, salvo nei casi espressamente previsti dalla legge.

Negli ordinamenti irlandese, italiano e maltese, l'anonimizzazione rimane applicabile nei procedimenti a porte chiuse (diritto irlandese), così come nei procedimenti in cui è possibile l'identificazione di minori (diritto italiano e maltese), o di vittime di determinati reati, in particolare di reati sessuali (diritto irlandese, italiano e maltese), oppure riguarda le decisioni relative al diritto di famiglia (diritto italiano) o contenenti dati sensibili (diritto irlandese e italiano).

Tuttavia, va segnalato che negli ordinamenti irlandese e maltese, il giudice ha un potere discrezionale molto ampio per quanto riguarda la scelta di anonimizzare una decisione al momento della pubblicazione.

Per quanto riguarda l'Italia è necessario apportare qualche precisazione [19]. In effetti, sebbene l'Italia faccia parte della categoria di ordinamenti giuridici in cui la pubblicità dei dati è la regola, ci sono tuttavia delle eccezioni, quali l'anonimato in determinati procedimenti penali ovvero su richiesta dell'interessato per motivi legittimi, o anche d'ufficio, a tutela dei diritti o della dignità degli interessati. Tali regole avvicinano l'ordinamento italiano agli ordinamenti giuridici appartenenti alla terza categoria (ibidem punto 3.1.3.) in cui l'anonimato è applicato solo a determinate cause o ad alcune modalità di pubblicazione.

---

[19] Si veda al riguardo, G. Grasso, *Il trattamento dei dati di carattere personale e la riproduzione dei provvedimenti giudiziari*, in *Foro it.*, 2018, V, 349, ed anche dello stesso autore, *Il trattamento dei dati di carattere personale e la riproduzione dei provvedimenti giudiziari: dal Codice della privacy all'attuale disciplina*, Scuola Superiore della magistratura, Corte di Appello di Bari, 25 ottobre 2019; P. Patatini e F. Troncone, *L'oscuramento dei dati personali nei provvedimenti della Corte Costituzionale*, in *Servizio Studi della Corte Costituzionale*, dicembre 2020, ed infine M. Van Opijnen, G. Peruginelli, E. Kefali, M. Palmirani, *On-line publication of court decisions in the EU*, "Report of the Policy Group of the Project 'Building on the European Case Law Identifier", 15 febbraio 2017.

È vero che, in linea generale, la pubblicità degli atti è la regola. L'articolo 51, secondo comma, del codice della privacy[20] prevede infatti che «le sentenze e le altre decisioni dell'autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet [...]».

Tuttavia, l'articolo 52 dello stesso codice prevede che l'omissione dei dati anagrafici possa essere disposta dall'autorità giudiziaria su richiesta dell'interessato, per motivi legittimi (1 comma), ovvero anche d'ufficio, a tutela dei diritti o della dignità degli interessati (2 comma), in ogni caso di loro riproduzione, in qualsiasi forma, da chiunque disposta. Inoltre, il divieto di diffusione dei dati identificativi si applica anche in assenza di decreto dell'autorità che ha pronunciato la sentenza o adottato il provvedimento, sia nelle ipotesi previste dall'art. 734-*bis* c.p. relativamente alle persone offese da atti di violenza sessuale, sia ogniqualvolta è possibile desumere anche indirettamente l'identità di minori, oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone, e quando riguarda dati, pure se relativi a terzi, dai quali è possibile risalire all'identità delle precisate persone.

Al di fuori dei casi in cui sia disposta l'anonimizzazione o debba procedersi all'oscuramento dei dati, la diffusione integrale delle decisioni giudiziarie di ogni ordine e grado è sempre consentita, anche attraverso la pubblicazione da parte dell'autorità giudiziaria su internet e l'inserimento in banche dati (articolo 52, settimo comma). Le decisioni giudiziarie nazionali sono così pubblicate su diversi database. In particolare nell'archivio ItalgiureWeb – il cui accesso è circoscritto a un numero definito di utenti (magistrati, pubblica amministrazione, avvocati, università e biblioteche, con accesso riservato o su abbonamento) – è possibile trovare sia le decisioni dei giudici italiani (in particolare della Corte di Cassazione e della Corte Costituzionale) in versione integrale, sia delle Corti sovranazionali (Corte di Giustizia dell'Unione europea e Corte europea dei diritti dell'uomo). All'inverso, per la pubblicazione delle massime delle decisioni civili vengono oscurati automaticamente tutti i nomi delle parti a prescindere da una richiesta di anonimizzazione, sia con

[20] Decreto legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali (modificato dal decreto legislativo 10 agosto 2018, n. 101 – 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 94/46/CE (regolamento generale sulla protezione dei dati).

riferimento alle persone fisiche sia con riguardo agli enti e alle persone giuridiche. Le sentenze integrali collegate alle massime contengono invece tutti i dati personali delle parti, se non oscurati ai sensi dell'art. 52 del codice della privacy. Le massime penali contengono invece il riferimento al nome dell'imputato e questo riferimento costituisce, nell'ambito penale, uno dei criteri per identificare e citare i precedenti.

Riguardo all'archivio SentenzeWeb della Corte di Cassazione, accessibile al pubblico, l'attuale limitazione della diffusione delle sentenze per un periodo massimo di cinque anni, con l'automatica rimozione di quelle che, a causa del trascorrere del tempo, risultino non più ricomprese nel suddetto ambito temporale, risponde all'esigenza di garantire il rispetto del diritto alla cancellazione dei dati. Anche in tale archivio, le sentenze contengono tutti i dati personali delle parti, che non siano stati oscurati ai sensi dell'art. 52 del codice della privacy.

3.1.3. L'anonimato applicato solo nelle procedure incardinate dinanzi ad alcuni organi giudiziari

In un terzo gruppo di ordinamenti, esiste un principio di anonimizzazione che si applica solo a determinati organi giudiziari o in considerazione delle modalità di pubblicazione.

Questo gruppo comprende undici ordinamenti giuridici (diritto belga, croato, cipriota[21], spagnolo, francese, lettone, lituano, polacco, rumeno, sloveno e ceco). In dieci di questi ordinamenti, il campo di applicazione di tale principio è piuttosto ampio, in quanto riguarda tutti i Tribunali supremi, ad esclusione delle Corti Costituzionali (diritto croato, ceco, francese, lettone, lituano, polacco, rumeno, sloveno, spagnolo e cipriota). Anche nel diritto belga[22], l'anonimizzazione si applica solo alle decisioni della Corte di Cassazione e alle decisioni del Consiglio di Stato in materia di diritto degli stranieri.

Laddove si applica il principio dell'anonimato, esso trova essenzialmente gli stessi tipi di limiti alla sua applicazione presenti negli ordinamenti appartenenti al primo gruppo. Sono dunque escluse dall'anonimizzazione le persone giuridiche (diritto belga, cipriota, spagnolo, francese, lettone, lituano[23] e ceco), le autorità pubbliche (diritto rumeno e ceco), le pronunce in determinate materie,

[21] Ai sensi del diritto cipriota, anche dopo l'attuazione del GDPR, tutte le decisioni pronunciate dalla Corte suprema nella sua veste di Corte Costituzionale non sono anonimizzate.

[22] Secondo il diritto belga, l'anonimizzazione delle decisioni della Corte Costituzionale è disposta d'ufficio o su richiesta.

[23] Secondo la legge lituana, tuttavia, i nomi delle società possono essere resi anonimi se costituiscono un segreto ai sensi della legge.

come il diritto dei marchi (diritto sloveno), così come è esclusa l'anonimizzazione qualora possa pregiudicare la corretta comprensione della decisione (diritto lettone, sloveno e ceco).

Allo stesso modo, per i Tribunali dinanzi ai quali la regola generale è l'assenza di anonimato, sono previste delle eccezioni che prevedono la protezione dei minori o delle vittime di determinati reati (si veda, in particolare, il diritto spagnolo). È prevista, inoltre, la possibilità di anonimizzazione su richiesta (diritto belga, spagnolo e ceco) o sulla base della natura specifica di alcuni rimedi costituzionali (diritto croato, francese[24], polacco[25] e sloveno[26]).

In diritto estone, il principio dell'anonimato si applica normalmente solo nelle procedure penali, ma non riguarda i dati relativi alle persone accusate di un reato, tranne nel caso in cui si tratti di minori. Inoltre, il principio si estende ad alcune tipologie di cause civili e amministrative[27].

Con riguardo al diritto francese, è opportuno sottolineare che, grazie ad una recente riforma del 2019 che ha modificato il codice dell'organizzazione giudiziaria e il codice di giustizia amministrativa[28], l'anonimizzazione si applica alla pubblicazione di tutte le decisioni giudiziarie nei formati elettronici. Anche le decisioni diffuse nel formato cartaceo ed accessibili ai terzi che ne fanno richiesta sono rese anonime se vi è il rischio di violare la sicurezza o la *privacy* delle persone interessate.

---

[24] Secondo il diritto francese, i nomi delle persone fisiche che sono parti di un procedimento su una questione prioritaria di costituzionalità sono resi anonimi.

[25] Nel diritto polacco, l'anonimato si applica solo alle decisioni sull'ammissibilità delle domande presentate alla Corte Costituzionale.

[26] La legge slovena garantisce l'anonimato, tra l'altro, nelle controversie relative all'esame delle domande presentate alla Corte Costituzionale per le quali è prevista una procedura a porte chiuse.

[27] Si può notare che, secondo la legge estone di attuazione del GDPR, nei procedimenti giudiziari sia civili che amministrativi, se l'anonimato è richiesto da una delle parti del procedimento, il giudice non ha la possibilità di rifiutare l'anonimato della relativa decisione giudiziaria.

[28] Loi n. 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice régissent la publication et l'anonymisation des décisions de justice disponibile al link : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038261631/. Si veda inoltre il décret n. 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives che applica le disposizioni dell'articolo 33 della legge precitata e disponibile al link : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042055251#:~:text=des%20juridictions%20...-,D%C3%A9cret%20n%C2%B0%202020%2D797%20du%2029%20juin%202020%20relatif,des%20juridictions%20judiciaires%20et%20administratives&text=Publics%20concern%C3%A9s%20%3A%20juridictions%20judiciaires%20et,auxiliaires%20de%20justice%20et%20justiciables.

3.2. Le regole di designazione delle decisioni giudiziarie

In quasi tutti gli ordinamenti, l'anonimizzazione viene effettuata sostituendo i nomi delle parti e, il più delle volte, quelli delle altre persone fisiche menzionate nella decisione, con le loro iniziali (diritto tedesco, austriaco, belga[29], bulgaro, croato, spagnolo[30], greco[31], ungherese, irlandese, italiano, lituano, polacco, slovacco, svedese e ceco), o, in alcuni casi, con iniziali fittizie (diritto croato, danese, estone, finlandese, francese, italiano, lettone, maltese, portoghese, rumeno e sloveno) o un nome fittizio (diritto spagnolo[32]). In alcuni casi, i sono anche utilizzati termini neutri come "richiedente" (diritto tedesco, austriaco, ungherese, olandese e sloveno). Nell'ordinamento cipriota, i nomi e i soprannomi delle parti sono oscurati, ma i loro cognomi sono mantenuti. Nell'ordinamento ceco, il nome dei minorenni viene sostituito da uno pseudonimo. Nell'ordinamento sloveno, invece, il nome di un richiedente asilo è talvolta sostituito dalle iniziali seguite dall'indicazione del suo paese d'origine.

In un numero significativo di ordinamenti, la portata dell'anonimizzazione va oltre i nomi delle parti e delle altre persone fisiche coinvolte e si estende a tutta una serie di altri dati che consentono di identificare una persona, come indirizzi e date (è questo il caso dell'ordinamento ceco, austriaco, belga[33], bulgaro, cipriota, croato, danese, estone, francese, greco, italiano, lettone, lituano, lussemburghese, olandese, polacco, portoghese, rumeno, slovacco, sloveno, spagnolo, svedese, tedesco e ungherese). A volte si estende anche ai rappresentanti delle parti e ai testimoni (diritto tedesco e croato) o solo a questi ultimi (diritto cipriota, spagnolo, francese, greco, lussemburghese e sloveno). In Francia, a partire dalla riforma del 2019, viene altresì anonimizzato qualsiasi elemento che consenta di identificare i giudici e i membri della cancelleria qualora la loro divulgazione rischi di mettere a repentaglio la loro sicurezza o la *privacy*.

Va notato, tuttavia, che in quasi tutti gli ordinamenti il principio è che, laddove è previsto l'anonimato, esso non riguarda la versione originale della decisione notificata alle parti. Solo due ordinamenti giuridici (belga e italiano) derogano, talvolta, a tale principio.

---

[29] Questa pratica è seguita in Belgio dalla Corte Costituzionale e dalla Corte di Cassazione.

[30] Questa è la prassi della Corte Costituzionale spagnola.

[31] Nel diritto greco, tale pratica non è sistematica.

[32] Questa pratica è attuata da Tribunali diversi dalla Corte Costituzionale spagnola.

[33] Nel diritto belga, tale possibilità di anonimizzazione è applicata solo in caso di necessità.

3.3. Il regime nazionale applicato alla pubblicazione delle domande pregiudiziali

Le procedure di anonimizzazione appena descritte riguardano anche la pubblicazione delle domande pregiudiziali nello Stato di provenienza. In questa sezione saranno presentati i regimi di anonimizzazione sia degli Stati membri che pubblicano le domande pregiudiziali in internet (3.3.1.), sia di quelli che limitano o escludono tale pubblicazione (3.3.2.).

3.3.1. L'anonimizzazione negli Stati membri che pubblicano in internet le domande di pronuncia pregiudiziale

Nella stragrande maggioranza degli ordinamenti giuridici esaminati nello studio della Direzione Ricerca e Documentazione, le domande di pronuncia pregiudiziale delle Corti supreme sono pubblicate in internet (diritto austriaco, belga, bulgaro, cipriota, croato, ceco, danese, estone, finlandese, francese, greco, italiano, lituano, lussemburghese, olandese, polacco[34], sloveno, spagnolo, svedese, tedesco).

Tuttavia, la pubblicazione in internet presenta talvolta alcune peculiarità o limitazioni. Ad esempio, in Estonia, in deroga al principio di non pubblicazione delle ordinanze processuali, tutte le ordinanze contenenti domande di pronuncia pregiudiziale sono pubblicate. Nell'ordinamento svedese vengono pubblicate dalle Corti supreme solo le domande pregiudiziali, talvolta precedute da una sintesi. Allo stesso modo, sebbene le ordinanze siano pubblicate solo su decisione del giudice, questa è considerata la regola per le decisioni delle Corti supreme.

Negli ordinamenti esaminati sembra che il regime generale che disciplina l'anonimizzazione delle decisioni giudiziarie al momento della loro pubblicazione sia applicabile alle domande di pronuncia pregiudiziale. Così, in undici Stati membri, il principio dell'anonimato si applica, di norma, a tutte le domande di pronuncia pregiudiziale pubblicate, indipendentemente dalla Corte che ha deferito la causa (Austria, Bulgaria, Cipro, Danimarca, Finlandia, Germania, Grecia, Lussemburgo, Paesi Bassi, Polonia e Svezia). Nei restanti nove Stati membri, l'anonimizzazione delle domande di rinvio pubblicate non è sistematica, sia perché limitata ad alcune Corti supreme, con esclusione della Corte Costituzionale (Belgio[35], Croa-

[34] In linea di principio, in Polonia, la pubblicazione riguarda solo le domande di pronuncia pregiudiziale presentate dalla Corte suprema.

[35] Nel diritto belga, l'esclusione sistematica dell'anonimato si applica anche alle decisioni emesse dal Consiglio di Stato, tranne che nelle cause sui diritti degli stranieri.

zia, Spagna, Francia[36], Lituania, Slovenia[37] e Repubblica ceca) o ad alcune materie (Estonia), sia perché è in linea di principio esclusa (Italia). Tuttavia, in Italia, sono previste garanzie per assicurare, in via eccezionale, l'anonimato di alcune persone, in particolare nei casi relativi allo status delle persone o che coinvolgono minori, dato che l'anonimato è disposto dal giudice ed è previsto dalla legge.

3.3.2. L'anonimizzazione negli Stati membri che limitano o escludono la pubblicazione in internet delle domande di pronuncia pregiudiziale

Alcuni ordinamenti (sette in totale) limitano o escludono la pubblicazione in internet delle domande di pronuncia pregiudiziale. In cinque Stati membri (Ungheria, Irlanda, Malta, Portogallo[38] e Romania) tale pubblicazione è del tutto esclusa, pertanto la questione dell'anonimizzazione diventa irrilevante. Va notato che in Irlanda e Portogallo[39] questa mancanza di pubblicazione è dovuta alle regole secondo cui solo le decisioni giudiziarie finali sono pubblicate, il che esclude quindi le domande di pronuncia pregiudiziale.

Nei restanti due ordinamenti (Lettonia e Slovacchia), la limitazione o l'esclusione della pubblicazione in internet delle domande di pronuncia pregiudiziale può avvenire per motivi diversi. In Lettonia, ad esempio, la pubblicazione è lasciata alla discrezione del Tribunale, poiché si tratta di una decisione adottata nel corso del procedimento e non di una sentenza definitiva soggetta all'obbligo di pubblicazione. Per quanto riguarda la Slovacchia, la mancata pubblicazione delle domande di pronuncia pregiudiziale è prevista da disposizioni che non includono tali domande nella categoria delle decisioni che richiedono la pubblicazione. La pubblicazione sembra quindi essere lasciata alla discrezione del Tribunale. Quando, in rari casi, i rinvii pregiudiziali sono comunque pubblicati, questi due Stati membri applicano le loro regole generali sull'anonimato. Ad esempio, la legge slovacca garantisce l'anonimato, mentre la legge lettone lo limita alle domande della Corte suprema, escludendo quelle della Corte Costituzionale.

---

[36] Nel diritto francese è tuttavia garantita l'anonimizzazione dei nomi delle persone fisiche che sono parti di una procedura dinanzi al Consiglio Costituzionale.

[37] Il diritto sloveno, tuttavia, garantisce l'anonimato, in particolare per le decisioni emesse nelle controversie relative all'esame delle domande presentate dinanzi alla Corte Costituzionale, per le quali è prevista una procedura a porte chiuse.

[38] In Portogallo, tuttavia, l'assenza di pubblicazione in internet delle domande di pronuncia pregiudiziale sembra essere limitata alle Corti supreme.

[39] In Portogallo, questa spiegazione vale solo per le Corti supreme.

4. Conclusioni

L'evoluzione delle tecnologie informatiche e dei mezzi di comunicazione hanno imposto di rivedere le regole e le pratiche di pubblicazione delle decisioni giudiziarie.

Se l'esigenza dell'accesso alla giustizia impone di non limitare in modo arbitrario e distorto la diffusione della giurisprudenza, la necessità della protezione dei dati personali ha costretto a riconsiderare la portata di tale principio.

L'anonimizzazione, e dunque l'oscuramento dei nomi propri, si presenta come il giusto compromesso tra queste esigenze opposte, di accesso alla giustizia e di protezione dei dati personali degli individui coinvolti.

Il presente studio mette in evidenza che molti passi in avanti sono stati compiuti, ma che il trattamento dei dati non è uniforme, sussiste infatti una certa varietà nella definizione dell'ambito di applicazione delle regole sull'anonimizzazione ed anche nelle modalità di oscuramento dei dati.

Possiamo immaginare che l'evoluzione delle tecniche di intelligenza artificiale che permettono l'anonimizzazione automatica dei nomi consentirà di estendere tali pratiche, talvolta gravose, e allo stesso tempo di uniformizzarne le procedure[40].

Non si può dunque che auspicare che, in un futuro prossimo, queste evoluzioni tecniche creeranno i presupposti per una disciplina comune in tutti gli Stati membri.

[40] A tal riguardo è utile menzionare il nuovo strumento d'intelligenza artificiale utilizzato dalla Corte di Cassazione e dal Consiglio di Stato francese Lab IA (Etalab) al fine di anonimizzare automaticamente le decisioni giudiziarie (per un approfondimento (in francese): https://transformations-droit.com/webinaire-la-pseudonymisation-des-decisions-de-justice-travaux-du-lab-ia-avec). È opportuno segnalare che anche in seno al gruppo interistituzionale "e-Justice" si sta discutendo l'uso dell'intelligenza artificiale per l'anonimizzazione nella diffusione delle decisioni nelle versioni elettroniche (vedi a tal punto la Strategia in materia di giustizia elettronica 2019-2023 (2019/C 96/04), disponibile al link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:C:2019:096:FULL&from=EN).

Edoardo Buonvino

Il dato personale nei provvedimenti giurisdizionali in materia civile, contenziosa e di volontaria giurisdizione. Circolazione dei provvedimenti ed esigenza di riservatezza delle persone cui essi si riferiscono

Sommario: 1. La base normativa del trattamento dei dati personali ad opera dell'autorità giudiziaria. – 2. La circolazione dei provvedimenti giurisdizionali e dei dati personali in essi contenuti. – 3. La circolazione "necessaria" per la protezione della persona vulnerabile. Il caso dell'amministrazione di sostegno.

1. La base normativa del trattamento dei dati personali ad opera dell'autorità giudiziaria

L'evoluzione normativa e, in parte, giurisprudenziale, che ha caratterizzato l'ultimo ventennio ha, visto un progressivo passaggio da una concezione tradizionale, per cui, essendo il *proprium* del processo costituito dalla pubblicità, lo spazio per la tutela del diritto alla riservatezza doveva essere necessariamente residuale (e quantitativamente assai limitato), ad una, più recente, ansia da anonimizzazione estrema, tale da travolgere non solo prassi consolidate, ma anche da porre in dubbio la concreta applicazione di norme di legge processuale vigenti.

La funzione "sociale" del diritto alla riservatezza, ne determina la non assolutezza, essendovi senza dubbio eccezioni al suo riconoscimento, come già Stefano Rodotà evidenziava ancor prima che la *privacy* trovasse codificazione nel nostro ordinamento. Peraltro, la possibilità di una compressione della riservatezza è elemento non nuovo alla tradizione europea. Basti pensare all'art.8 della Convenzione europea dei diritti dell'uomo, che stabilisce che "non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che l'ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, alla difesa e alla prevenzione dei reati". Inoltre, la Convenzione del Consiglio d'Europa n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale consente (all'art. 11) deroghe specifiche alle disposizioni generali in tema di riservatezza, se necessarie, "per la protezione della sicurezza e difesa nazionale, della sicurezza

pubblica, dell'imparzialità e indipendenza della magistratura o la prevenzione, indagine e repressione di condotte criminali e l'esecuzione delle pene.

Lo stesso GDPR contiene, nella sua parte generale, alcune disposizioni che costituiscono esplicazione della funzione sociale del diritto alla riservatezza. L'art. 6, ad esempio, fissando le condizioni di liceità del trattamento di dati personali, elenca, oltre al consenso dell'interessato, e in via di alternativa, diversi ulteriori possibili presupposti, quali la necessità di salvaguardare interessi vitali dell'interessato o di altra persona, la necessità del trattamento per eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Con riferimento ai dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati relativi ala salute alla vita o all'orientamento sessuale della persona, il cui trattamento è, in generale, vietato, le possibili eccezioni sono relative alla necessità di trattamento per motivi di interesse pubblico "rilevante sulla base del diritto dell'Unione o degli Stati Membri", a condizione che il trattamento sia proporzionato alla finalità perseguita, rispetti l'essenza del diritto alla protezione dei dati, e preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Non stupisce, quindi, che l'art. 23, §1 lett. f) del GDPR stabilisca la possibilità, per gli Stati membri, di limitare "mediante misure legislative" la portata degli obblighi e dei diritti stabiliti dal Regolamento al fine di salvaguardare l'indipendenza della magistratura e dei procedimenti giudiziari, l'esecuzione (*enforcement,* da intendersi, quindi, come esecuzione in senso tecnico) delle azioni civili (*claims*). Avvalendosi di tale deroga il legislatore interno ha dunque introdotto l'art. 2 *duodecies* del Codice Privacy, che disciplina il perimetro della limitazione, nonché l'ambito soggettivo e le finalità della limitazione stessa.

Le disposizioni derogate sono, segnatamente, quelle contenute negli artt. da 12 a 22 e nell'art. 34 del Codice. Esse riguardano i diritti dell'interessato e l'obbligo di tempestiva comunicazione dell'eventuale compromissione dei dati trattati, quando essa sia suscettibile di determinare un rischio elevato per i diritti e le libertà delle persone fisiche. L'art. 2 *duodecies* del Codice Privacy, introdotto in applicazione del GDPR stabilisce, infatti, che "in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonché' dinanzi al Consiglio superiore della magistratura e agli altri organi di autogoverno delle magistrature speciali o presso il Ministero della giustizia, i diritti e gli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento sono disciplinati nei limiti e con le modalità previste dalle disposizioni di legge o di Regolamento che regolano tali procedimenti, nel rispetto di quanto previsto dall'articolo 23, paragrafo 2, del Regolamento".

Prosegue la norma specificando che "in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonché' dinanzi al Consiglio superiore della magistratura e agli altri organi di autogoverno delle magistrature speciali o presso il Ministero della giustizia, i diritti e gli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento sono disciplinati nei limiti e con le modalità previste dalle disposizioni di legge o di Regolamento che regolano tali procedimenti, nel rispetto di quanto previsto dall'articolo 23, paragrafo 2, del Regolamento."

Con riferimento all'oggetto del trattamento, le deroghe in esame sono estese a tutte le tipologie di dati personali, da non confondersi con i dati giudiziari, vale a dire quelli relativi alle condanne penali e ai reati o alle connesse misure di sicurezza.

Le disposizioni interne mantengono, peraltro, una delimitazione delle eccezioni alle norme generali fondata anche sul criterio soggettivo, tecnica, questa, abbandonata dal GDPR ma tuttora consentita ai legislatori nazionali. È stata, quindi, sostanzialmente ripresa l'indicazione data dall'ormai abrogato art. 46 del codice privacy, con l'indicazione, quali titolari del trattamento, gli uffici giudiziari i ogni ordine e grado, i rispettivi apparati amministrativi nonché gli ausiliari del giudice, gli organi di autogoverno delle magistrature speciali, oltre al CSM, e il Ministero della giustizia.

Sotto il profilo oggettivo, sono interessati dalla deroga i procedimenti che si svolgono di fronte agli organi appena elencati. La disposizione in esame circoscrive ulteriormente l'area dell'eccezione, specificando che si intendono effettuati per ragioni di giustizia i trattamenti di dati personali **correlati alla trattazione giudiziaria di affari e di controversie**, i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonché i trattamenti svolti nell'ambito delle attività ispettive su uffici giudiziari. Le ragioni di giustizia non ricorrono per l'ordinaria attività amministrativo-gestionale di personale, mezzi o strutture, quando non è pregiudicata la segretezza di atti direttamente connessi alla trattazione giudiziaria di procedimenti.

2. La circolazione dei provvedimenti giurisdizionali e dei dati personali in essi contenuti

Ciò premesso in ordine alla fonte normativa della liceità del trattamento dei dati personali ad opera dell'autorità giudiziaria, si vogliono esaminare le questioni pratiche attinenti alla pubblicità di questioni prendenti e di provvedimenti giurisdizionali e, più, in generale, ai profili concernenti la "circolazione" dei provvedimenti medesimi.

Si tratta di aspetti regolati dagli artt. 51 e 52 del Codice Privacy, aventi ad oggetto, l'uno, l'accesso ai dati identificativi dei procedimenti pendenti, l'altro la diffusione del contenuto, anche integrale, di sentenze ed altri provvedimenti.

L'accesso anche ai soli dati identificativi è consentito ai portatori di un interesse, genericamente indicato, ed il cui contenuto deve essere ricavato in via interpretativa. Parte della dottrina ha ritenuto che il richiamo generico vada interpretato distinguendo tra pubblicità nei confronti delle parti e nei confronti di terzi. Nel primo caso, infatti, andrebbe garantita la massima trasparenza al fine di non pregiudicare l'esercizio del diritto di difesa. Per i terzi, al contrario, l'interesse è suscettibile di valutazione a seconda del tipo di procedimento e della fase in cui esso si trova[1].

L'art. 52, rubricato "dati identificativi degli interessati", disegna due possibili modalità di salvaguardia del diritto alla riservatezza. In particolare, l'interessato, "può chiedere, per motivi legittimi, con richiesta depositata in cancelleria o segreteria dell'ufficio che procede, prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato, riportati sulla sentenza o provvedimento". Sulla richiesta provvede, l'autorità che pronuncia la sentenza o adotta il provvedimento, con decreto in calce. Il secondo comma dell'art. 52 dispone, inoltre, che la medesima autorità possa disporre d'ufficio l'apposizione dell'annotazione del comma 1, "a tutela dei diritti o della dignità degli interessati".

In ogni caso, a prescindere dalla apposizione della "clausola", il comma 5 del richiamato articolo 52 dispone che "chiunque diffonde sentenze o altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado è tenuto ad omettere in ogni caso, (…) le generalità, altri dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità dei minori oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone.

Il settimo comma del citato articolo precisa, infine, che, fuori dei casi indicati dalle disposizioni che lo precedono, "è ammessa la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali".

È, dunque, ben sottolineato che il principio generale, quando si tratta di sentenze e altri provvedimenti giurisdizionali, non è quello della riservatezza, ma quello della massima diffusione.

---

[1] Scarano, *Sub art. 51* in Bianca e Busnelli, *La protezione dei dati personale, Commentario al d.lgs.30 giugno 2003 n.196,* Padova, 2007.

Le disposizioni in esame richiedono, si ritiene, un giudizio di bilanciamento volto a stabilire l'opportunità della limitazione del principio generale di liceità della diffusione del contenuto delle sentenze e degli altri provvedimenti. Il Garante della *privacy*, nelle linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica, del 2 dicembre 2010, ha osservato che, i motivi legittimi di opposizione alla diffusione potrebbero essere individuati in relazione alla "delicatezza della vicenda oggetto del giudizio" o alla "particolare natura dei dati contenuti nel provvedimento". In particolare, l'autorità dovrebbe disporre l'anonimizzazione qualora vengano in rilievo "dati personali dotati di particolare significatività che, se indiscriminatamente diffusi, possono determinare negative conseguenze sui vari aspetti della vita sociale e di relazione dell'interessato (ad esempio in ambito familiare e lavorativo).

A tale proposito è bene sottolineare che le indicazioni del garante sono riferite alla riproduzione di provvedimenti per finalità di informazione giuridica, posto che, all'epoca della loro pubblicazione, il codice privacy si riferiva puntualmente alla diffusione di provvedimenti, appunto, per finalità di informazione giuridica su riviste giuridiche, supporti elettronici, o mediante reti di comunicazione elettronica. Con il nuovo art. 52 l'inciso è stato eliminato, e, tuttavia, l'abrogazione parziale non sembra avere mutato sostanzialmente la disciplina applicabile.

Ciò premesso, si è visto come, fuori dai casi di omissione dei dati identificativi specificamente indicati nell'art. 52, non vigono particolari divieti di diffusione in relazione ai provvedimenti adottati.

3. La circolazione "necessaria" per la protezione della persona vulnerabile. Il caso dell'amministrazione di sostegno.

Vi è, però, un profilo che merita ulteriore approfondimento in questa sede, concernente la attitudine – per così dire – necessaria alla circolazione di determinati provvedimenti contenenti dati personali e sensibili, senza possibilità di oscuramento dei dati identificativi. Non dunque, sacrificio della riservatezza a generali esigenze di trasparenza o informazione, nell'ambito meramente processuale, ma diffusione necessaria del provvedimento giurisdizionale per la tutela della persona stessa cui i dati si riferiscono.

Si pensi in primo luogo, ai procedimenti in tema di amministrazione di sostegno.

Come noto, l'amministrazione di sostegno si apre a beneficio della persona che, per infermità fisica o psichica, non è in grado di attendere efficacemente ai propri interessi. La particolarità dell'amministrazione di sostegno rispetto ai tradizionali istituti codicistici è data principalmente dalla sua flessibilità, vale a dire dalla atipicità dei poteri attribuiti all'amministratore di sostegno, in via di mera assistenza alla persona beneficiaria o mediante l'attribuzione di un vero e

proprio potere sostitutivo, relativamente al compimento di un singolo atto, o di un una o più categorie di atti, che possono riguardare tanto la sfera patrimoniale quanto quella personale.

L'amministratore di sostegno, pertanto, al fine di poter esercitare il proprio ufficio, rappresentando il beneficiario nei rapporti con i terzi, deve poter giustificare il proprio potere mediante esibizione del decreto di apertura dell'amministrazione, delle sue successive modifiche, nonché di eventuali ulteriori decreti, che abilitino l'amministratore al compimento di singole attività, non previste dal decreto "generale".

I terzi con cui venga a contatto l'amministratore, dunque, avranno necessità di esaminare ed interpretare il decreto che viene loro sottoposto a giustificazione del potere rappresentativo di volta esercitato dall'amministratore medesimo, verificando se, per l'atto da compiere, il beneficiario abbia mantenuto, ad esempio, inalterata la propria capacità di agire, o se debba essere assistito, ovvero, ancora, sostituito integralmente.

Ora, è del tutto evidente che i provvedimenti in esame contengono, anche solo nella parte dispositiva, tutta una serie di indicazioni idonee a rivelare l'identità, le condizioni di salute, ivi comprese eventuali menomazioni fisiche o psichiche, e, a seconda dei casi, anche la vita o l'orientamento sessuale della persona.

È del tutto fisiologico, ad esempio, che nel decreto che chiude la fase "eventualmente contenziosa" ed apre quella gestoria dell'amministrazione, vengano date all'AdS disposizioni concernenti tanto la rappresentanza negoziale (ivi compreso, ad esempio, l'onere di rappresentare il beneficiario nelle assemblee condominiali) quanto l'elaborazione e l'attuazione di un piano terapeutico, di cui è sempre opportuno che vengano indicate, nel decreto, quantomeno le finalità.

Nella generalità dei casi, quindi, l'amministratore di sostegno, al fine di svolgere correttamente il proprio ufficio, dovrà necessariamente esibire il decreto, contenente le più varie informazioni personali, a svariate categorie di destinatari (si pensi, ad esempio, ad operatori bancari e creditizi, pubbliche amministrazioni, privati prestatori di servizi, soci e dipendenti di associazioni e società, amministratori di condominio, condòmini, operatori di servizi telefonici, finanche negozianti titolari di attività al dettaglio).

Tali persone hanno non solo l'interesse, ma anche l'onere di verificare che i poteri che l'amministratore pretende di esercitare in luogo dell'amministrato corrispondano a quelli attribuitigli dal giudice, essendo, in caso contrario, esposti quantomeno all'azione di annullamento degli atti negoziali compiuti dal rappresentante privo dei relativi poteri, salva un'eventuale responsabilità risarcitoria. Ai fini di tale verifica, e anche al fine di acquisire una prova documentale per tenersi a riparo da eventuali, successive, contestazioni, il terzo avrà necessità non solo

di farsi esibire, ma, a seconda dei casi, anche di acquisire in copia, il decreto di apertura dell'amministrazione o il diverso provvedimento autorizzativo che venga in rilievo a seconda dei casi.

Poiché, poi, tali provvedimenti devono necessariamente essere motivati in relazione alle condizioni di salute fisica o psichica della persona interessata, è assolutamente probabile che una notevole quantità di informazioni e dati personali anche irrilevanti rispetto alla prestazione del servizio che venga di volta in volta in rilievo venga comunicata ad un elevato numero di soggetti.

Si pensi all'ipotesi del beneficiario di amministrazione di sostegno che soffra di una patologia psichica incidente, in ipotesi, anche sulla sfera sessuale, e per il quale l'amministratore di sostegno sia stato incaricato di redigere un piano terapeutico, ma anche, ad esempio, di partecipare ad assemblee condominiali in rappresentanza del beneficiario medesimo.

In casi come quello delineato, che nella pratica sono tutt'altro che infrequenti, l'amministratore di sostegno sarà costretto ad esibire all'amministratore di condominio il decreto di nomina, che conterrà anche le indicazioni sul progetto terapeutico da predisporre ed attuare. L'amministratore di condominio, poi, prudentemente dovrà acquisire una copia del decreto in questione, così dando origine ad un ulteriore trattamento di dati personali, peraltro, non così strettamente collegato allo svolgimento di attività giurisdizionale da sottrarsi ai vincoli generali di cui al Codice Privacy e al GDPR. In caso di successive contestazioni in ordine alla validità della deliberazione, poi, il decreto di apertura potrebbe dover essere esibito agli altri condomini, così dando luogo ad un'ulteriore diffusione.

La problematicità della situazione emerge in modo ancora più chiaro se si considera che i decreti di apertura, devono essere, come ogni provvedimento giurisdizionale, motivati, e, in particolare, devono esserlo in relazione alle patologie fisiche e psichiche che specificamente impediscono alla persona beneficiaria di compiere determinati atti, lasciando, invece, intatta la sua capacità di compierne altri.

Ancora più critica si rivela la situazione se si considera che la diffusione di dati personali non è destinata ad esaurirsi nel contesto di un unico esercizio dei poteri dell'ads, ma è generalmente destinata a ripetersi per ogni successiva occasione di intervento dell'amministratore, per tutto l'arco di vita della persona amministrata.

Ora, l'esercizio dei poteri rappresentativi attribuiti all'amministratore di sostegno non può essere ritenuto un trattamento compiuto nell'esercizio della funzione giurisdizionale, né costituisce, in senso proprio, esecuzione di una sentenza o di altro provvedimento. L'amministratore, infatti, non adempie, normalmente a specifiche disposizioni del giudice tutelare, ma esercita un potere rappresentativo attribuitogli in maniera più o meno ampia. La base giuridica del trattamento e

per la comunicazione dei dati personali non sembra poter essere costantemente ricercata nella lett. f) dell'art. 9 del GDPR, anche in considerazione del fatto che il successivo art. 23, §1, lett. f) si riferisce ai trattamenti effettuati "nell'ambito di procedimenti dinanzi agli uffici giudiziari", e non alla comunicazione all'esterno, da parte di soggetti estranei all'amministrazione della giustizia, dei dati acquisiti nell'ambito di quei procedimenti.

L'art. 9 del GDPR prevede che il divieto di trattare dati personali che, tra l'altro, rivelino dati relativi alla salute o alla vita sessuale della persona interessata, non si applichi quando (lett. c) "il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso". Tale presupposto, tuttavia, non sempre si verifica in tema di amministrazione di sostegno, posto che, in tema di amministrazione di sostegno, vige il principio per cui il beneficiario conserva integra la propria capacità di agire, salvo che in relazione agli specifici atti indicati dal giudice tutelare nel decreto con cui la misura viene disposta. Pertanto, in mancanza della specifica indicazione, da parte del giudice tutelare, della perdita della capacità di agire da parte del beneficiario in relazione alla prestazione del consenso relativo al trattamento dei dati personali di cui all'art. 9 del Regolamento, appare difficile ricondurre l'attività dell'amministratore di sostegno alla specifica previsione normativa.

Potrebbe argomentarsi che il trattamento e la comunicazione di dati sia fondato, quanto all'attività svolta dall'amministratore, sulla base della lett. g) dell'art. 9, che consente il trattamento quando esso sia necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Qualche perplessità, sul punto, viene, tuttavia, dall'esame dell'art. 6, §3 lett. b) del GDPR (che, peraltro, riguarda in generale il trattamento dei dati e non solo quello di quelli specificamente indicati all'art. 9, secondo cui la finalità del trattamento), secondo cui la base giuridica in esame "potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del (presente) regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento, le tipologie di dati oggetto del trattamento, gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto" (…).

Con specifico riguardo alla materia dell'amministrazione di sostegno, sebbene sia indubbia la finalità di interesse pubblico del trattamento dei dati, non solo

quello eseguito nell'ambito del procedimento avanti all'ufficio giudiziario, ma anche quello compiuto dall'amministratore nell'esercizio della propria pubblica funzione, è evidente come manchino disposizioni di legge tese a disciplinare gli obblighi che l'amministratore di sostegno deve osservare nel trattamento dei dati e, in particolare, nella loro comunicazione a terzi.

A tale proposito va sottolineato che il problema potrebbe porsi in modo meno intenso qualora l'amministratore fosse un professionista, posto che egli sarebbe tenuto, già per altro verso, al rispetto di una nutrita serie di obblighi relativi al trattamento dei dati, tuttavia, statisticamente, sono ben più frequenti le circostanze in cui l'incarico di amministrazione viene affidato a soggetti non professionisti.

Inoltre, stante la particolarità dei connotati del procedimento per amministrazione di sostegno, che è stato definito come un abito sartoriale, specificamente tagliato sulle esigenze del singolo beneficiario, è anche difficile immaginare un modello "standard", valido per tutti i casi e in tutte le condizioni.

Per questo, nella pratica quotidiana, ricade sui giudici l'individuazione di un bilanciamento accettabile tra garanzia della riservatezza della persona beneficiaria e necessità di consentire all'amministratore la piena esplicazione dei suoi poteri.

Una prima, basilare, forma di bilanciamento, comunemente attuata dai giudici tutelari, consiste nella disposizione, rivolta all'amministratore di sostegno, di esibire ai terzi, al fine di giustificare i propri poteri, il decreto di apertura nella sola parte dispositiva, e non, invece, in quella motiva. Si tenta, in questo modo, di ridurre al minimo la diffusione di dati relativi alla salute della persona, necessariamente presenti nella parte motiva, e che, invece, più agevolmente possono essere omessi nella parte dispositiva.

Vi è, però, da osservare, che tale accorgimento, da un lato non sempre è sufficiente ad evitare la diffusione e l'ulteriore trattamento di dati personali, posto che essi, come si è visto, ben possono essere contenuti anche nel dispositivo del provvedimento di apertura.

D'altro canto, va considerato che il "mascheramento" dell'intera parte motiva del provvedimento, sebbene autorizzato dallo stesso giudice che lo ha emesso, qualora operato direttamente dall'amministratore di sostegno, soggetto privo di poteri certificativi, priva la copia esibita del requisito della conformità all'originale, sicché, in assenza di precise disposizioni di legge in merito, il terzo potrebbe ritenere non giustificata la spendita del nome del beneficiario da parte dell'amministratore di sostegno e frapporre ostacoli alla pur doverosa attività dell'amministratore di sostegno.

Sotto il profilo pratico, talune cancellerie hanno adottato l'accorgimento di rilasciare copie autentiche dei decreti in esame già totalmente oscurate nella

parte motiva. In questo modo il soggetto cui venga esibito il decreto da parte dell'amministratore di sostegno, al fine di giustificarne i poteri, è posto in grado di verificare l'esistenza della "delega", senza, tuttavia, poter conoscere la motivazione del provvedimento. Sotto il profilo pratico non risulta che gli amministratori di sostegno abbiano incontrato particolari difficoltà ai fini del riconoscimento del loro potere rappresentativo, sicché il bilanciamento individuato potrebbe ritenersi soddisfacente. Rimane, tuttavia, il dubbio se, in punto di diritto possa ritenersi fino a tal punto sacrificabile l'aspettativa di colui al quale il provvedimento viene esibito di conoscerne la motivazione e se il terzo medesimo, posto di fronte ad un provvedimento orbato della sua motivazione, non possa, invece, pretendere che questa gli venga quantomeno esibita, eventualmente anche al fine di contestare (anche in sede giurisdizionale) l'attribuzione di poteri all'amministratore, nei limiti in cui tale legittimazione gli spetti.

Anche a prescindere, comunque, dalla comunicazione a terzi del decreto, l'attività rappresentativa (o anche solo di assistenza) svolta dall'amministratore di sostegno nei limiti stabiliti dal decreto che stabilisce la misura di protezione appare poco o per nulla disciplinata dalla legge quanto ai profili concernenti il trattamento, la comunicazione e l'eventuale diffusione di dati personali riguardanti il beneficiario. Come anche in altri casi, la giurisprudenza si è fatta carico di individuare possibili forme di tutela della riservatezza e di bilanciamento delle opposte esigenze che, peraltro, riguardano la medesima persona beneficiaria, la quale, per il semplice fatto di essere tale, si trova in posizione di particolare vulnerabilità. Il rischio derivante dal riempimento del vuoto normativo da parte della giurisprudenza, tuttavia, è quello della mancanza di quello standard minimo che consentirebbe un maggiore affidamento sul fatto che sia assicurato alle persone vulnerabili il minor sacrificio possibile del loro diritto alla riservatezza. Rimane, quindi, auspicabile che le modalità di trattamento e comunicazione dei dati, da parte di amministratori di sostegno, curatori e tutori, venga presa in considerazione dal legislatore, così da dare un assetto stabile alla materia.

Martina Flamini

Ttutela civile della persona e dell'identità

Sommario: 1. Premessa. – 2. Rapporto tra procedimento amministrativo e procedimento giurisdizionale: la portata del principio di alternatività di cui all'art. 140-*bis* del c.d. Nuovo Codice della Privacy. – 3. La tutela della persona dinanzi al Garante e dinanzi al Giudice: esame di un caso. – 4. Il rimedio della deindicizzazione globale: la posizione del Garante e quella del Giudice Ordinario alla luce della giurisprudenza europea.

1. Premessa

"*Senza una forte tutela delle informazioni che le riguardano, le persone rischiano sempre di più d´essere discriminate per le loro opinioni, credenze religiose, condizioni di salute: la privacy si presenta così come un elemento fondamentale dalla società dell´eguaglianza. Senza una forte tutela dei dati riguardanti le convinzioni politiche o l´appartenenza a partiti, sindacati, associazioni, i cittadini rischiano d´essere esclusi dai processi democratici: così la privacy diventa una condizione essenziale per essere inclusi nella società della partecipazione. Senza una forte tutela del "corpo elettronico", dell´insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo diventa così evidente che: la privacy è uno strumento necessario per difendere la società della libertà, e per opporsi alle spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale*".

Il rapporto tra privacy, libertà e dignità era al centro delle parole pronunciate dal prof. Stefano Rodotà nel discorso conclusivo della Conferenza internazionale sulla protezione dei dati (Polonia, settembre 2004).

E proprio sul rapporto tra trattamento dati, identità e dignità si concentra il presente contributo che si propone un'analisi del rapporto tra forme di tutela amministrativa e giurisdizionale, compiuta attraverso l'analisi di alcune decisioni assunte dalle corti italiane e sovranazionali.

Il taglio del mio intervento e le funzioni da me svolte (giudice addetto alla Sezione del Tribunale di Milano che si occupa di diritti della persona e, in particolare, di diritto al lecito trattamento dei dati personali) spiegano le ragioni di

una trattazione che non si soffermerà sui molti aspetti teorici già approfonditi da attenta dottrina[1], ma sugli aspetti pratici emersi nei procedimenti esaminati.

2. Rapporto tra procedimento amministrativo e procedimento giurisdizionale: la portata del principio di alternatività di cui all'art. 140-*bis* del c.d. Nuovo Codice della Privacy

Per comprendere in che termini si atteggi la tutela amministrativa del diritto alla protezione dati ed in che modo si atteggi, invece, la tutela giurisdizionale, è necessario soffermarsi sulla tipologia di poteri e rimedi della pubblica amministrazione.

In primo luogo, occorre chiarire la natura dei provvedimenti emessi dall'Autorità Garante.

La Suprema Corte (Cass. 20 maggio 2002, n. 7341) ha da tempo affermato che l'ordinamento non conosce un *tertium genus* tra amministrazione e giurisdizione, alle quali la Costituzione riserva rispettivamente, per distinguerne e disciplinarne le attività, gli art. 111 e 97 e che non vi è nel sistema costituzionale una figura di paragiurisdizionalità a sé stante, distinta dalle due predette. Ritenuti non dirimenti i requisiti relativi all'oggetto del decidere (giacché alle pubbliche amministrazioni è dato di provvedere su diritti in forme definite giustiziali dalla dottrina), all'interesse pubblico costituente il riferimento fondamentale del giudice (atteso che la P.A. provvede in considerazione di un interesse pubblico generale) ed al rispetto del contraddittorio, la Corte di Cassazione – anche in ossequio al disposto dell'art. 29, comma 7, della legge n. 675 del 1996 (con disposizione ora prevista all'art. 10, comma 6, del d.lgs. 150/2011), in forza della quale il Tribunale adito in opposizione alla decisione del Garante provvede anche in deroga al divieto di cui all'art. 4 della legge 2248 del 1865, all. E – ha accertato la natura amministrativa (e non giurisdizionale) dell'organo e del relativo procedimento, che non pone il Garante nella stessa posizione di terzietà assicurata dal giudice nel processo (cfr. Cass. 20.5.2002 n. 7341/2002 e Cass. 25.6.2004 n. 11864).

In merito a tale aspetto, la Corte di Cassazione ha poi precisato che: "il ricorso al Giudice ordinario in opposizione al provvedimento del Garante non può essere inteso che come primo rimedio giurisdizionale a disposizione del soggetto che si pretende leso dall'atto del Garante" (Cass. 25.5.2002 n. 7341).

---

[1] S. Rodotà, *Tecnologie e diritti*, 1995; V. Cuffaro, V. Ricciuto, V. Zeno Zencovich (a cura di), *Trattamento dati e tutela della persona,* 1999; G. Resta, *Autonomia privata e diritti della personalità. Il problema dello sfruttamento economico degli attributi della persona in prospettiva comparatistica*, Napoli, 2005; C. Angiolini, *Lo Statuto dei dati personali*, Pisa, 2020.

Le controversie in esame non si configurano come gravame, rispetto al provvedimento adottato dal Garante in sede amministrativa, ma come opposizione, ed è proprio la natura amministrativa della fase svoltasi dinanzi al Garante che determina l'inidoneità del provvedimento emesso all'esito a passare in giudicato (cfr. Cass. 25.05.2017 n. 13151; Cass. 18.6.2018 n. 16061).

L'art. 58 del Reg. 2016/678 specifica ed individua le tre tipologie dei poteri di indagine, dei poteri correttivi e dei poteri consultivi ed autorizzativi.

Il ruolo e i poteri delle autorità garanti sono state affrontate in dettaglio nel caso Weltimmo C-230/14, in cui la CGUE si trovava ad affrontare la questione relativa alla possibilità che l'autorità ungherese per la protezione dei dati potesse esercitare il potere, conferitole dalla legge ungherese, di infliggere un'ammenda ad una società che, pur essendo registrata in Slovacchia, gestiva un sito web per il commercio immobiliare riguardante proprietà site in Ungheria. Il rinvio pregiudiziale si riferiva in realtà alla questione circa il campo di applicazione territoriale della legge, e se l'autorità ungherese avrebbe potuto esercitare i propri poteri contro una società registrata in Slovacchia. Tuttavia, la Corte ha ritenuto che, prima di trattare l'ambito di applicazione territoriale dei dati nazionali poteri dell'autorità di protezione, "è necessario esaminare quali sono i poteri di tale autorità di controllo". Alla luce dell'articolo 28, paragrafi 1, 3 e 6, della direttiva 95/46".

Per la Corte, dall'art. 28, n. 1, della direttiva 95/46 risulta che ciascuna autorità di controllo stabilito da uno Stato membro deve garantire il rispetto, all'interno del territorio di tale Stato membro, con le disposizioni adottate in applicazione della direttiva 95/46. Inoltre la Corte osserva che, ai sensi dell'art. 28, n. 3, della direttiva 95/46, tali autorità di controllo si trovano a essere dotati in particolare di poteri investigativi, quali i poteri di raccolta di tutte le informazioni necessari per l'esercizio delle loro funzioni di vigilanza e di effettivi poteri d'intervento, quali come potere di ordinare il blocco, la cancellazione o la distruzione dei dati, di imporre un'azione temporanea o il divieto definitivo di trattamento o di avvertire o ammonire il responsabile del trattamento dei dati. La Corte sottolinea che tale elenco di poteri non deve essere considerato esaustivo e che, tenuto conto del tipo di potere discrezionale di cui dispongono gli Stati membri in materia di recepimento della direttiva 95/46, si deve considerare che tali poteri di intervento possono comprendere il potere di sanzionare il responsabile del trattamento dei dati imponendogli, se del caso, un'ammenda. La Corte aggiunge che tale potere dovrebbe essere esercitato conformemente al diritto processuale dello Stato membro a cui appartiene l'autorità di controllo.

Nel più recente caso Holstein C-210/16, la CGUE riprende i principi affermati in Weltimmo per affermare che la competenza può essere esercitata dall'autorità garante dello Stato membro in cui la società responsabile del trattamento è sta-

bilita, anche non è il soggetto che opera concretamente il trattamento all'interno del gruppo societario, ma soltanto quello che opera la vendita di spazi pubblicitari e le altre attività di *marketing*.

Se le autorità di vigilanza devono cooperare tra loro nella misura necessaria per l'esecuzione del progetto dei loro compiti, in particolare attraverso lo scambio di tutte le informazioni utili, tale direttiva non prevede criteri di priorità che disciplinano l'intervento di un'autorità di vigilanza rispetto ad un'altra, né prevede l'obbligo per un'autorità di controllo di uno Stato membro di rispettare la posizione che può essere stata espressa dall'autorità di controllo di un altro Stato membro. Le autorità nazionali di controllo sono responsabili, ai sensi dell'articolo 8, paragrafo 3, CDF e l'articolo 28 della direttiva 95/46, per il controllo del rispetto delle norme UE concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali. Come conseguenza, a ciascuno di essi è conferito il potere di verificare se il trattamento dei dati personali nel territorio del proprio Stato membro soddisfa i requisiti stabiliti dalla direttiva 95/46.

Nel Regolamento 2016/679 i poteri delle autorità di controllo indipendenti sono definiti in modo più ampio. Tra questi, il potere di "imporre un'ammenda amministrativa ai sensi dell'articolo 83, in aggiunta o in luogo delle misure di cui al presente paragrafo, a seconda delle circostanze di ogni singolo caso" è esplicitamente indicato come potere obbligatorio per le autorità di controllo.

Il legislatore dell'UE ha pertanto tenuto conto dell'esito del dialogo giudiziario svoltosi in seno alla CGUE in decisioni, come quelle qui commentate, in cui la Corte ha interpretato esplicitamente o implicitamente la direttiva 95/46 alla luce del principio di effettività. Attualmente questo principio è esplicitamente menzionato all'articolo 83 del Regolamento, insieme ai principi di proporzionalità e dissuasività (par. 1).

L'art. 140-*bis* del Codice Privacy fissa il principio dell'alternatività secondo il quale

a) il ricorso al Garante non può essere proposto se per il medesimo oggetto e tra le stesse parti è stata già adita l'autorità giudiziaria;
b) la presentazione del reclamo al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto, salvo quanto previsto dall'articolo 10, comma 4, del decreto legislativo 1° settembre 2011, n. 150.

L'alternatività riguarda esclusivamente le domande aventi un identico oggetto, ovvero quelle che, se pendenti contestualmente davanti a più giudici, possono, in via generale, essere assoggettate al regime processuale della litispendenza o della continenza. Si tratta delle domande che richiedono interventi di natura preventiva, inibitoria o conformativa, potendo il Garante indicare modalità concrete di cessazione del trattamento illecito dei dati. La domanda di risarcimento

del danno patrimoniale o non patrimoniale ha *causa petendi* e *petitum* radicalmente divergenti da quelle sopra esaminate ed è destinata ad una declaratoria d'inammissibilità se proposta davanti al Garante. Peraltro, in numerose pronunce (*ex multis* 19/2/2002 doc. web. 1063674; 5 ottobre 2006 doc. web. 135919), il Garante ha ritenuto inammissibile il ricorso contenente una domanda risarcitoria, ritenendosi privo di competenza al riguardo.

Tale principio presuppone che le domande si riferiscano alle stesse parti ed abbiano identico oggetto (cioè che si tratti di "domande che se pendenti contestualmente davanti a più giudici possono, in via generale, essere assoggettate al regime processuale della litispendenza o della continenza": Cass. 17.9.2014 n. 19534).

Come chiaramente affermato dalla Suprema Corte, "l'accoglimento del ricorso, totale o parziale, da parte del Garante può, in conclusione, facilitare il ricorso alla tutela risarcitoria davanti all'autorità giudiziaria ordinaria, ma non escluderla. Diversamente ragionando, dovrebbe ritenersi alternativamente che scelta la strada della tutela inibitoria (e preventiva), sia negata quella risarcitoria, oppure che, nonostante il riconoscimento del trattamento illecito dei dati personali, la parte sia tenuta ad un'impugnazione del provvedimento del Garante al solo fine di richiedere il risarcimento del danno e non incorrere nella sanzione di tardività dell'azione. Quest'ultima soluzione è in netto contrasto con il canone costituzionale della ragionevolezza. La prima introduce un impedimento all'ottenimento della tutela piena di un diritto fondamentale quale quello in gioco, del tutto incompatibile con l'art. 24 Cost.. Diversa è la soluzione in caso di rigetto del ricorso da parte del Garante. In tale ipotesi, condicio sine qua non per adire l'autorità giudiziaria è l'impugnazione tempestiva del provvedimento di diniego, con conseguente facoltà di proporre la connessa domanda risarcitoria unitamente a quella relativa all'accertamento della illiceità del trattamento dei dati" (Cass. 17.9.2014 n. 19534; cfr. anche Cass. Sez. lav. 7.4.2016 n. 6775).

La Suprema Corte si è più volte occupata del rapporto tra il ruolo dell'autorità di controllo e quello dei tribunali nei procedimenti giudiziari. In particolare, con sentenza del 12.10.2012 n. 17408 la Corte ha affrontato la questione chiarendo che l'alternativa tra i due meccanismi di esecuzione non impone nel caso specifico che l'azione giudiziaria debba essere dichiarata inammissibile, essendo quest'ultima iniziata prima della richiesta all'autorità di protezione dei dati. Nel caso specifico, sono i procedimenti dinanzi all'autorità di controllo che avrebbero dovuto essere considerati inammissibili. Tuttavia, dato che la decisione dell'autorità per la protezione dei dati è stata presa prima della conclusione del procedimento giudiziario e non è stata impugnata dalle parti, essa ha solo l'effetto relativo alle argomentazioni delle parti, vale a dire che la decisione dell'autorità di controllo non può essere discussa dalle parti dinanzi al giudice.

Con pronuncia del 25.5.2017 n. 13151, la Corte suprema ha affrontato l'impatto della decisione dell'autorità nazionale di controllo nei confronti del procedimento giudiziario relativo al risarcimento dei danni. Dato che la decisione del tribunale può essere emessa anche in un altro procedimento in un momento successivo al ricorso dinanzi all'autorità nazionale di controllo per quanto riguarda la violazione delle norme sulla protezione dei dati, la Corte suprema ha affermato che **la decisione dell'autorità di controllo non può vincolare il tribunale civile in quanto una tale decisione non acquisirà mai lo status (e avrà gli effetti) di cosa giudicata**, dato che l'autorità di protezione dei dati è un organo amministrativo e la sua procedura garantisce l'imparzialità dell'autorità di protezione dei dati come quella garantita dal tribunale in un procedimento giudiziario.

Con riferimento alla giurisprudenza europea, sul rapporto relativo alla sequenzialità fra ricorso amministrative e giudiziario merita di essere ricordata la decisione della CGUE nel caso Puškár, C-73/16.

Il sig. Puškár è una persona fisica che ha presentato un ricorso alla Corte Suprema della Repubblica slovacca chiedendo che la Direzione Finanza, tutti gli uffici fiscali sotto il suo controllo e la Direzione Finanze Ufficio amministrativo penale di rimuovere il suo nome da un elenco, precedentemente redatto dalla Direzione Finanza, dei responsabili delle posizioni direttive all'interno delle aziende. Sebbene il sig. Puškár avesse affermato che tale elenco poteva circolare solo tra gli uffici amministrativi, tale elenco conteneva il suo Numero di Identità e Codice Fiscale costituendo un violazione dei suoi diritti e quindi il sig. Puškár chiedeva la rimozione del suo nome e di ogni riferimento a lui dall'elenco e da altri elenchi analoghi, nonché dal sistema informatico dell'autorità finanziaria. La Corte suprema ha respinto la domanda poiché il sig. Puškár non aveva esaurito i rimedi dinanzi alle autorità amministrative nazionali. Il sig. Puškár ha quindi presentato ricorso alla Corte Costituzionale della Repubblica slovacca.

La Corte Costituzionale slovacca si è concentrata principalmente sulla giurisprudenza relativa all'articolo 6, paragrafo 1, della CEDU in relazione all'articolo 46 della Costituzione slovacca. La Corte si è occupata in particolare dell'obbligo dei tribunali di giustificare la loro decisione tenendo conto di tutti i fatti e gli elementi giuridici pertinenti. Tale obbligo è stato considerato una condizione preliminare per l'esercizio del diritto delle parti a un ricorso effettivo. In questo senso, la Corte Costituzionale ha affermato che per soddisfare i requisiti dell'articolo 46 Cost. (e dell'articolo 6 della CEDU), l'analisi della Corte suprema avrebbe dovuto tener conto di tutte le circostanze del caso rispetto al livello di protezione dei dati personali garantito dall'articolo 46 Cost. Costituzione e il livello di protezione della *privacy* garantito dalla CEDU. Così, la Corte Costituzionale ha concluso che la Corte suprema non aveva preso in considerazione gli argomenti di fatto e di diritto e, cosa più importante, aveva mancato di fornire una decisione in merito a

quali condizioni la protezione dei dati personali avrebbe dovuto essere rispettata nel caso del trattamento dei dati da parte delle autorità fiscali. La Corte Costituzionale ha poi affermato che la Corte suprema ha violato i diritti fondamentali del ricorrente, vale a dire il diritto a un ricorso effettivo e a un processo equo, il diritto alla *privacy* e il diritto alla protezione dei dati personali. Pertanto, la Corte Costituzionale ha rinviato la causa alla Corte suprema.

A questo punto, la Corte suprema, ritenendo che la Corte Costituzionale non avesse tenuto conto della giurisprudenza della Corte di Giustizia dell'Unione europea, ha deciso di adire tale Corte per una pronuncia pregiudiziale.

La prima questione mirava a verificare se il procedimento amministrativo preliminare obbligatorio adottato dal legislatore slovacco nel caso in questione fosse conforme al diritto dell'UE e in particolare all'articolo 47 CDF.

Dopo aver dichiarato che i dati personali raccolti a fini fiscali rientrano nell'ambito di applicazione della direttiva n. 95/46, poiché sono trattate dall'articolo 13, paragrafo 1, di tale direttiva, la CGUE inizia ad esaminare ciascuna delle questioni pregiudiziali.

Per quanto riguarda la prima questione pregiudiziale, la Corte ricorda che l'obbligo di esaurire i rimedi amministrativi, pur non esclusi dalla direttiva n. 95/46, devono essere esaminati alla luce dell'Articolo 47 CDF, articolo 4, paragrafo 3 del TUE (principio di leale cooperazione) e articolo 19, paragrafo 1 del TUE (principio di leale cooperazione). il TUE (tutela giurisdizionale effettiva nei settori coperti dal diritto dell'UE). Poiché l'obbligo di esaurire i mezzi di ricorso amministrativi supplementari costituisce una limitazione del diritto ad un'effettiva il ricorso giurisdizionale può essere giustificato secondo i criteri stabiliti a norma dell'articolo 52 (1) CFREU, ossia solo quando:

i) previsto dalla legge;
ii) rispettoso dell'essenza del diritto;
iii) nel rispetto del principio di proporzionalità;
iv) rispettare gli obiettivi di interesse generale riconosciuti dall'UE o la necessità di tutelare i diritti dei cittadini europei, diritti e libertà altrui.

La Corte si è concentrata in particolare sugli ultimi due criteri. Per quanto riguarda l'esistenza di obiettivi di interesse generale, la Corte ha riconosciuto che l'obbligo di presentare un reclamo amministrativo prima di avviare un'azione legale ha due principali aspetti positivi effetti: in primo luogo, può sollevare le giurisdizioni da controversie che possono essere decise in tempi più brevi dinanzi al Tribunale di primo grado; e, in secondo luogo, può aumentare l'efficienza dell'autorità giudiziaria. Pertanto, l'obbligo generale persegue obiettivi di interesse generale. Per quanto riguarda il test di proporzionalità, la Corte si è basata sul parere dell'AG e sulle decisioni di Alassini e Menini. In particolare, ha fatto esplicito riferimento ai criteri individuati nella decisione Alassini (par. 67) che

dovrebbe orientare il test di proporzionalità rispetto alle fasi aggiuntive imposte dalla procedura nazionale, vale a dire

1. Le procedure non danno luogo ad una decisione vincolante per le parti,
2. Le procedure non causano un ritardo sostanziale ai fini dell'introduzione di un'azione legale. Procedure,
3. I procedimenti sospendono il termine di prescrizione,
4. Le procedure non danno luogo a costi – o a costi molto bassi – per le parti,
5. La procedura non sono previste solo per via elettronica,
6. Le procedure prevedono misure provvisorie in casi eccezionali in cui l'urgenza della situazione lo richiede.

L'esame dei poteri dell'autorità di controllo e dell'autorità giudiziaria, in materia di tutela conseguente alle violazioni del diritto alla protezione dei dati personali, nonché l'analisi della tipologia dei provvedimenti emessi evidenzia come l'autorità giudiziaria – anche quando venga adita in sede di opposizione avverso i provvedimenti del Garante – sia sovente chiamata alla scelta di un rimedio che, nel rispetto dei principi di effettività e proporzionalità, garantisca una tutela effettiva.

3. La tutela della persona dinanzi al Garante e dinanzi al Giudice: esame di un caso (Trib. Milano, 15.1.2020)

Il tema del delle forme di tutela civile della persona e dell'identità, oggetto del presente intervento, può essere affrontato a partire dall'analisi di un caso in cui le soluzioni offerte dall'autorità amministrativa e da quella giurisdizionale hanno portato ad esiti differenti.

Con ricorso *ex* art. 152 d.lgs. 196/2003, i ricorrenti, in proprio e quali genitori adottivi esercenti la potestà genitoriale su una ragazza minorenne, hanno evocato in giudizio, dinanzi al Tribunale di Milano, l'Autorità Garante per la Protezione dei dati personali, chiedendo di ordinare, anche *inaudita altera parte*, al Garante di disporre, ordinandola al titolare della pagina di un noto s*ocial network* la immediata rimozione/blocco di tutti i messaggi "postati" dal padre biologico della minore, allorchè idonei ad indentificare, anche con l'ausilio di terzi, le ragazze adottate e a rintracciare le medesime ed il nucleo familiare adottivo, sussistendo i presupposti di cui all'art. 700 c.p.c..

A sostegno del ricorso, hanno dedotto: che il Tribunale per i minorenni di Milano aveva disposto farsi luogo all'adozione delle minori; che una delle due giovani, nelle more divenuta maggiorenne, accedendo al proprio profilo aperto sul *social network*, dopo aver digitato il proprio nome e la propria data di nascita, era stata indirizzata sul profilo personale del padre biologico; che tale collega-

mento era stato reso possibile dal fatto che quest'ultimo aveva postato alcuni messaggi, sulla propria bacheca pubblica contenenti dati personali delle figlie adottive, idonee ad identificarle e diretti a reperire informazioni volte a riprendere i contatti con loro; che i ricorrenti si erano rivolti al Centro assistenza *on line* del *social network*, che aveva rifiutato di procedere alla rimozione; che, con segnalazione del 19.3.2019, i ricorrenti si erano rivolti all'Autorità Garante per la Protezione dei Dati personali, al fine di ottenere il blocco e il divieto di diffusione *on line* dei contenuti predetti, ritenuti atti di *cyberbullismo*; che, con provvedimento reso il 10 maggio 2019, il Garante aveva rigettato le istanze spiegate dagli odierni ricorrenti, ritenendo che la fattispecie non apparisse riconducibile nè alle disposizioni di cui alla legge. 71 del 29.5.2017 né all'ambito di applicazione in materia di dati personali "trattandosi di vicenda che appare richiedere, nei termini nei quali è stata posta, l'intervento dell'autorità giudiziaria che ha emesso il provvedimento di adozione"; che tutti i post contenenti i dati identificati delle due giovani erano ancora liberamente accessibili; che entrambe le ragazze, dopo aver appreso dei tentativi di ricerca da parte del padre biologico, vivevano in uno stato di prostrazione psicologico, come confermato anche dalla relazione di una psicologa, depositata in atti.

Il Garante per la protezione dei Dati personali si è costituito deducendo: che, per integrare il fenomeno del *cyberbullismo* le condotte elencate dall'art. 1 della l.71/2017 dovevano essere caratterizzate, come espressamente previsto dalla legge, dallo scopo intenzionale e predominante di "isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso e la loro mesa in ridicolo"; che, nel testo del messaggio in esame, non era dato riscontrare i predetti requisiti; che il trattamento dei dati personali, seppure illecito (in quanto effettuato senza il consenso dei minori e dei genitori), non costituiva un atto di *cyberbullismo*; che nella segnalazione del 19.3.2019 i genitori adottivi non avevano richiesto l'adozione dei provvedimenti invocati alla luce delle disposizioni sul trattamento dei dati personali; che, pur volendo considerare la predetta segnalazione come un reclamo ai sensi dell'art. 77 del Regolamento 2016/679, gli interessati non erano comunque identificabili, in quanto la stessa era stata presentata nell'interesse di "genitori adottivi", senza l'indicazione delle loro generalità. Ha, dunque, concluso chiedendo il rigetto del ricorso, con vittoria di spese.

Nel provvedimento in esame il Tribunale di Milano, dopo aver escluso l'applicabilità della disciplina sul c.d. *cyberbullismo* (in ragione della diversità delle fattispecie esaminate) si è soffermata sulla possibilità di tutelare i diritti invocati in forza della disciplina sul trattamento dei dati personali (pure incidentalmente richiamata dal Garante).

L'art. 6 individua le basi giuridiche del trattamento. In particolare la norma in esame prevede: "*Il trattamento è lecito solo se e nella misura in cui ricorre alme-*

no una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è 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; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore".

L'art. 8 comma 1 prevede che: "*Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale*".

Il considerando 38 del GDPR prevede che: "i minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali".

Alla luce dei predetti principi, il Tribunale ha concluso che la protezione dei diritti inviolabili della persona costituisce il principale criterio che deve orientare l'interprete nell'esegesi del sistema normativo, e nel bilanciamento tra diritti fondamentali, per assicurare il rispetto della dignità della persona umana. Tale impostazione si rivela l'unica compatibile con il principio personalistico che anima la nostra Costituzione, la quale vede nella persona umana un valore etico in sé e vieta ogni strumentalizzazione della medesima per alcun altro fine eteronomo ed assorbente.

Con riferimento al caso di specie, il Tribunale di Milano ha ritenuto pacifica l'assenza di consenso della minore (e dei suoi genitori) alla divulgazione di dati relativi alla data e al luogo di nascita, alle generalità ed alle informazioni relative all'adozione. Né ha ravvisato, nel messaggio sopra indicato, la presenza delle altre basi giuridiche del trattamento. Deve ritenersi, pertanto, che la pubblicazione dei predetti dati, relativi ad un minore, integri un trattamento illecito dei dati personali.

In merito al fatto che autore del messaggio fosse il padre biologico della minore, il Tribunale, richiamate le disposizioni della legge 4.5.1983 n. 184 ha

evidenziato come spetti esclusivamente all'adottato – anche al momento della maggiore età, se sussistono "gravi e comprovati motivi attinenti alla sua salute psico-fisica" – il diritto di accedere alle informazioni relative alle proprie origini. Tale diritto, come ricordato dalla Corte Europea dei diritti dell'Uomo nella sentenza *Godelli c. Italia*, rientra nel perimetro della tutela offerta dall'art. 8 della Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, essendo protetto dalla Convenzione "l'interesse vitale... a ottenere delle informazioni necessarie alla scoperta della verità concernente un aspetto importante della propria identità personale, ad esempio l'identità dei propri genitori".

Nel caso in esame, invece, era il genitore biologico che, attraverso la divulgazione di dati personali sulla propria bacheca del profilo aperto sul *social network* – e dunque con modalità che hanno esposto la minore ad un'improvvisa, incondizionata ed incontrollata diffusione di informazioni relative alla propria identità personale, la cui tutela informa la disciplina sopra richiamata – ha cercato di accedere ad informazioni relative alle proprie figlie biologiche, da tempo adottate dagli odierni ricorrenti. Il trattamento dei dati della minore, pertanto, integra un trattamento dei dati personali di una minore che, in assenza di alcuna delle sei basi giuridiche, deve ritenersi illecito.

All'esito delle predette argomentazioni il Tribunale, dopo aver accertato che i messaggi presenti sulla bacheca pubblica del padre biologico della minore contengano dati personali delle figlie naturali che costituiscono un trattamento illecito dei dati personali delle predette, in riforma del provvedimento emesso dal Garante per la protezione dei dati personali il 10.5.2019, ha ordinato alla società responsabile per il trattamento dei dati dei cittadini europei la rimozione e il blocco di tutti i messaggi contenenti dati personali relativi alle figlie naturali e comunque idonei ad indentificarle.

Il rimedio della deindicizzazione globale: la posizione del Garante e quella del Giudice Ordinario alla luce della giurisprudenza europea.

L'esame del caso deciso dal Tribunale di Milano – in sede di reclamo, con ordinanza del 17.6.2020, avverso la decisione di accoglimento del ricorso *ex* art. 700 c.p.c. – pone l'interprete di fronte a numerose questioni da risolvere quali l'individuazione della situazione giuridica soggettiva lesa, la scelta tra i diversi mezzi di tutela, la decisione sulla competenza giurisdizionale e l'ammissibilità di un ordine di rimozione "globale".

Nel caso in esame, il ricorrente si era inizialmente rivolto al Garante per la protezione dei dati personali, lamentando la lesione della dignità e della reputazione (e, dunque, non la violazione del diritto al lecito trattamento dei dati personali) e chiedendo di ordinare la rimozione dal motore di ricerca Google di una lista di *link* contenenti notizie asseritamente false e lesive della sua dignità

e reputazione. Il Garante aveva accolto la richiesta di deindicizzazione globale degli URL indicati nel ricorso introduttivo, ritenendo sussistente il diritto all'oblio dell'interessato in forza dei principi affermati dalla Corte di Giustizia nella nota sentenza *Costeja*.

Avverso il provvedimento del Garante ha proposto ricorso il motore di ricerca in forza dei seguenti motivi: l'ordine di deindicizzazione globale costituiva un provvedimento che andava oltre il campo di applicazione della Direttiva 95/46/CE e travalicava i limiti del Trattato dell'Unione europea, che imponevano chiari limiti territoriali all'applicabilità delle leggi europee; un'eventuale deindicizzazione globale avrebbe avuto l'effetto di creare una "giurisdizione universale" e non avrebbe consentito di operare quel bilanciamento tra diritto all'oblio e libertà di informazione, che doveva avvenire sulla base delle leggi applicabili in ciascuno Stato membro; erroneamente il Garante aveva accolto il ricorso, sulla base di argomentazioni relative al diritto all'oblio, diverso dal diritto all'onore e alla reputazione, invocato dal ricorrente e tutelabile dinanzi al giudice ordinario e non all'autorità amministrativa; nel provvedimento impugnato vi era stata un'erronea interpretazione della sentenza della Corte di Giustizia e delle Linee Guida relative al bilanciamento tra diritto all'oblio e libertà di informazione.

In primo luogo, appare necessario soffermarsi sulle questioni in merito alla giurisdizione del giudice italiano adito per ottenere una tutela di diritti lesi via web, con contenuti visionabili dagli utenti di tutto il mondo.

Ad avviso del Tribunale di Milano, trattandosi di responsabilità da fatto illecito, deve trovare applicazione la disciplina del *forum commissi delicti,* contenuta nell'art. 5 n. 3 del Regolamento Bruxelles I (che è stata sostituita, a partire dal 10 gennaio 2015, dal corrispondente art. 7 n. 2 del Regolamento n. 1215/2012, che ne ha però mantenuto sostanzialmente invariata la formulazione letterale). Tale criterio di competenza giurisdizionale costituisce un foro non solo speciale e alternativo rispetto al foro generale del domicilio (o sede) del convenuto, ma anche facoltativo.

La Corte di Giustizia è più volte intervenuta, pronunciandosi in via pregiudiziale, sull'interpretazione dell'art. 5 n. 3 del Regolamento Bruxelles I, che ha sostituito la Convenzione di Bruxelles del 1968. La continuità, a livello interpretativo, tra l'articolo 5 n. 3 della Convenzione di Bruxelles e il corrispondente articolo contenuto nel Regolamento n. 44/2001 è stata sancita dal legislatore europeo nel diciannovesimo considerando del Regolamento Bruxelles I, nonché dalla Corte di Giustizia (secondo la quale l'interpretazione fornita con riferimento alle disposizioni della Convenzione di Bruxelles si estende anche a quelle del Regolamento del 2001 – e, *a fortiori*, del Regolamento Bruxelles I-*bis* -, nel caso in cui le disposizioni siano qualificabili come equivalenti).

Con riferimento alla nozione di "materia di delitto o quasi delitto", la Corte di Giustizia ne ha affermato, nella sentenza *Kalfelis,* il carattere di nozione europea autonoma, in cui è ricompresa «(...) qualsiasi domanda che miri a coinvolgere la responsabilità di un convenuto e che non si ricolleghi alla materia contrattuale di cui all'art. 5, n. 1».

La Corte di Cassazione ha più volte affermato che "ai fini di determinare l'ambito della giurisdizione italiana rispetto al convenuto non domiciliato né residente in Italia, occorre applicare i criteri stabiliti dalle sezioni 2", 3" e 4" del titolo 2 della Convenzione, anche quando il convenuto stesso sia domiciliato in uno Stato non contraente della Convenzione" (così Cass. S.U. ord. 21.10.2009 n. 22239; cfr. anche Cass. S.U. ord. 27.2.2008 n. 5090; Cass. S.U. ord. 11.2.2003 n. 2060, Cass. S.U. 12.04.2012, n. 5765).

Con riferimento al «luogo in cui l'evento dannoso è avvenuto» è ormai consolidata nella giurisprudenza europea il principio della piena dicotomia tra azione ed evento, secondo cui in caso di illeciti c.d. complessi o a distanza, caratterizzati dalla dissociazione geografica tra il luogo del fatto e il luogo del danno, è competente, a scelta dell'attore, sia il giudice del luogo del fatto generatore del danno (teoria dell'azione) sia il giudice del luogo in cui si è verificato il danno (teoria dell'evento).

La Corte di Cassazione ha da tempo ribadito come – esaminando la struttura dell'illecito disciplinato a livello comunitario ai soli fini di determinazione della competenza giurisdizionale – il criterio di collegamento debba essere individuato o **dal fatto generatore dell'illecito**, ovvero dal luogo ove si sia prodotta **la lesione diretta ed immediata** del bene protetto, ancorché gli effetti mediati dell'evento di danno possano diversamente propagarsi nel tempo e nello spazio (cfr. anche, per un'ampia ricostruzione della giurisprudenza comunitaria relativa all'interpretazione dell'art. 5 della Convenzione di Bruxelles, Cass. SS.UU. 5.7.2011 n. 14654).

Ancora, in via generale, mette conto osservare come il criterio di giurisdizione del "luogo in cui l'evento dannoso è avvenuto" debba essere interpretato facendo riferimento al centro di interessi del soggetto leso, e cioè il luogo della sua residenza abituale o dell'esercizio dell'attività professionale da parte della persona lesa (principi espressi dalla Corte di Giustizia con la sentenza 25.10.2011, C-509-9 – *eDate Advertising* e a. in un caso di diffamazione *on line*).

Nel caso esaminato dal Tribunale di Milano i giudici meneghini hanno ritenuto che la lesione possa ritenersi consumata nel luogo e nel momento in cui il soggetto leso abbia preso consapevolezza dei commenti denigratori postati sui profili del *social network*, consapevolezza che ha trovato concreta attuazione nel **paese di origine del danneggiato** (l'Italia).

Con riferimento alla qualificazione del diritto invocato, occorre precisare che l'individuazione della situazione giuridica soggettiva asseritamente lesa – diritto all'onore e alla reputazione, diritto alla tutela dei dati personali, o entrambi i diritti –, infatti, rileva:

a. sotto il profilo del quadro normativo di riferimento (per la tutela dei dati personali, infatti, vengono in rilievo l'art. 2 della Cost., l'art. 8 CEDU, l'art. 8 della Carta di Nizza ed il Reg. UE 679/2019), mentre per la tutela dell'onore e della reputazione si fa riferimento all'art. 2 della Cost., all'art. 8 CEDU e, con riferimento ai doveri dell'*hosting provider*, anche la Direttiva 31/2000 e il d.lgs. 70/2003);
b. con riferimento alla scelta dei rimedi (per la tutela dei dati personali l'art. 17 del Reg. 679/2019, mentre per la tutela dell'onore e della reputazione lesi attraverso condotte poste in essere nel mondo della rete, vengono in rilievo gli artt. 14 e 15 della Direttiva 31/2000, gli artt. 16 e 17 del D.lgs. 70/2003 e l'art. 21 della Cost.);
c. in merito all'individuazione dell'ambito di applicazione dei principi sanciti da Cass. S.S.U.U. n. 23469/2016 in tema di tutela cautelare nei confronti di contenuti diffamatori all'interno di testate giornalistiche online (che, come affermato dalla Suprema Corte, non si estende alla materia della protezione dei dati personali).

In merito ai rimedi esperibili, il Tribunale di Milano ha osservato come la direttiva 2000/31, in particolare il suo articolo 15, paragrafo 1, consenta che un giudice di uno Stato membro possa ordinare ad un servizio di *hosting* di rimuovere le informazioni oggetto dell'ingiunzione o di bloccare l'accesso alle medesime.

Con riferimento alla portata territoriale del predetto ordine, la Corte di Giustizia, nella sentenza *Eva Glawischning-Piesczek c. Facebook Ireland LT,* ha affermato che tale ordine può essere effettuato a livello mondiale, nell'ambito del diritto internazionale pertinente.

Come efficacemente chiarito nelle conclusioni dell'Avvocato Generale Maciej Szpunar presentate il 4.6.2019, nella causa C-18/18 (conclusosi con la pronuncia appena citata), il legislatore dell'Unione non ha armonizzato né le norme sostanziali in materia di pregiudizio alla vita privata e ai diritti della personalità, inclusa la diffamazione, né le norme di conflitto in materia (cfr. articolo 1, paragrafo 2, del regolamento (CE) n. 864/2007 del Parlamento europeo e del Consiglio, dell'11 luglio 2007, sulla legge applicabile alle obbligazioni extracontrattuali («Roma II», GU 2007, L 199, pag. 40). Pertanto, al fine di conoscere delle azioni di diffamazione, ciascun giudice dell'Unione ricorre alla legge designata come applicabile in forza delle norme nazionali di conflitto.

Nella diversa pronuncia della Corte di Giustizia (nella causa C-507/17, Google LLC /Commission nationale de l'informatique et des libertès, CNIL), invece, oggetto d'esame era la direttiva 95/46/CE, la quale armonizza, a livello dell'U-

nione – a differenza di quanto appena visto in materia di diffamazione – alcune norme sostanziali relative alla protezione dei dati.

Se, pertanto, il ricorrente si limiti ad invocare la tutela dell'onore e della reputazione, l'imposizione in uno Stato membro di un obbligo consistente nel rimuovere talune informazioni a livello mondiale (in conseguenza di un accertamento in fase sommaria), per tutti gli utenti di una piattaforma elettronica, a causa dell'illiceità di tali informazioni accertata in forza di una legge applicabile, avrebbe come conseguenza che l'accertamento del loro carattere illecito esplichi effetti in altri Stati (che ben potrebbero, secondo le norme nazionali di conflitto, ritenere invece leciti i contenuti oggetto di causa).

Tali considerazioni portano a ritenere che il giudice di uno Stato membro possa, in teoria, statuire sulla rimozione delle informazioni, manifestamente illecite, diffuse a mezzo Internet a livello mondiale. Tuttavia, come condivisibilmente sottolineato dall'Avvocato generale nelle richiamate conclusioni, "a causa delle differenze esistenti fra le leggi nazionali, da un lato, e la tutela della vita privata e dei diritti della personalità da esse prevista, dall'altro, e al fine di rispettare i diritti fondamentali ampiamente diffusi, un siffatto giudice deve adottare piuttosto un atteggiamento di autolimitazione".

Tale autolimitazione si realizza attraverso l'applicazione del principio di proporzionalità. Il diritto all'onore e alla reputazione non è un diritto assoluto, ma deve essere considerato in relazione alla sua funzione sociale ed essere bilanciato con altri diritti fondamentali, conformemente al principio di proporzionalità (in materia di trattamento dei dati personali, ma con argomentazioni che ben possono essere applicate nel caso di specie v., del pari, sentenza del 9 novembre 2010, Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, punto 48).

Non pare inutile ricordare che l'articolo 52, paragrafo 1, della Carta ammette che possano essere apportate limitazioni all'esercizio di diritti previsti dalla Carta stessa, purché tali limitazioni siano previste dalla legge, rispettino il contenuto essenziale di detti diritti e libertà e, nel rispetto del principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui (sentenza del 9 novembre 2010, Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, punto 50).

La nostra Corte Costituzionale, inoltre, ha affermato che nessun diritto fondamentale è protetto in termini assoluti dalla Costituzione, ma – al contrario – è soggetto a limiti per integrarsi con una pluralità di altri diritti e valori, giacché altrimenti si farebbe "tiranno" e porterebbe al totale annientamento di uno o più fattori in gioco (Corte Cost. 85/2013).

Una volta accertata la manifesta illiceità, nei contenuti postati in rete, nella scelta dei rimedi i giudici meneghini hanno ritenuto che, per assicurare al ricor-

rente una tutela effettiva, debba essere privilegiato il rimedio dal carattere fortemente incisivo, quale la rimozione definitiva dei contenuti.

Prima di esaminare il contenuto della decisione del Tribunale di Milano, non appare inutile ricordare che, proprio con riferimento al tema della portata del diritto alla de-indicizzazione, con provvedimento n. 557 del 21.12.2017 il Garante per la Privacy, ritenendo ammissibile un ordine di c.d. deindicizzazione globale, ha ordinato ad un motore di ricerca di rimuovere gli URL deindicizzati fra i risultati di ricerca ottenuti digitando il nome e cognome del ricorrente, sia nelle versioni europee che extraeuropee. Nel caso in esame, un professore universitario iscritto all'Anagrafe degli italiani residenti all'estero (AIRE) ha chiesto al Garante Privacy di ordinare a Google la deindicizzazione di 26 link, non limitata esclusivamente al territorio europeo, i quali si riferirebbero a contenuti gravemente offensivi della sua dignità e della reputazione. Il motore di ricerca, opponendosi al ricorso, ha evidenziato che la questione sulla deindicizzazione globale è attualmente all'esame della Corte di Giustizia dell'Unione europea nella causa C-507/17. Il Garante per la Privacy, accogliendo il ricorso, ha ritenuto che la perdurante reperibilità sul web dei contenuti indicati in ricorso avesse un impatto "sproporzionatamente negativo" sulla sfera del ricorrente, anche in ragione del trattamento di dati potenzialmente sensibili che lo riguardano, tanto da non poter essere considerati in linea con quanto disposto dall'art. 11 del Codice e dalle Linee Guida sull´attuazione della sentenza Costeja emanate dal WP29 il 26 novembre 2014. In ossequio al principio della tutela effettiva, e tenuto conto del fatto che il ricorrente risiedeva fuori dell'Unione europea, ha ritenuto opportuno estendere l´attività di rimozione degli URL in questione anche alle versioni extraeuropee del motore di ricerca. Il predetto provvedimento, impugnato dal motore di ricerca dinanzi al Giudice Ordinario, è stato riformato dal Tribunale di Milano che, con sentenza dell'11.7.2018 (sentenza n. 7846/2018), ha ritenuto insussistenti i presupposti per la tutela del c.d. diritto all'oblio del ricorrente (e dunque ha ritenuto non accoglibile l'istanza di deindicizzazione, a prescindere dalla questione relativa all'ambito territoriale del rimedio invocato).

Tornando al caso in esame, in merito all'estensione territoriale del rimedio della deindicizzazione, in applicazione del principio di proporzionalità, in ragione della tipologia di contenuti pubblicati, delle caratteristiche del soggetto denigrato (il quale non svolgeva alcun ruolo pubblico) e delle espressioni utilizzate (che in più parti fanno riferimento a vicende dal carattere privato), il Tribunale ha ritenuto che l'ordine di rimozione sia idoneo a garantire una tutela effettiva senza necessità di estensione a tutto il mondo.

Ancora in merito all'ambito territoriale di riferimento, il Tribunale di Milano ha osservato che la forte compressione della libertà di espressione – in Stati che, come evidenziato poco sopra, ben potrebbero prevedere discipline nazionali

diverse da quella dello Stato che emette l'ordine – conseguente ad un ordine di rimozione a livello mondiale richiede, proprio per il delicato bilanciamento tra diritti fondamentali, in ossequio a principi costituzionali e sovranazionali, l'intervento dell'autorità giudiziaria e difficilmente sembra demandabile a società private, quali i motori di ricerca o i *social network*.

In forza delle predette argomentazioni, il Tribunale di Milano ha ordinato al *social network* di rimuovere i contenuti manifestamente illeciti con riferimento ai soli Stati Europei, disattendendo la decisione del Garante che aveva, invece, previsto un ordine di rimozione globale.

L'esame dei casi appena condotta consente all'interprete di riflettere su alcune delle questioni che l'esigenza di tutela civile della persona e dell'identità pone in presenza di una lesione del diritto al trattamento dei dati personali. In particolare, occorrerà verificare la reale portata del diritto ad un ricorso giurisdizionale effettivo (art. 47 CDFUE) nel definire il rapporto tra tutela amministrativa e tutela giudiziaria. Atteso, infatti, che il citato art. 47 riguarda non solo il diritto degli individui, ma anche il rapporto tra tutela amministrativa, sarà compito dell'interprete verificare se il principio di alternatività sopra citato (art. 140-*bis*) costituisca uno strumento che garantisce all'interessato una tutela effettiva per verificare poi, in caso di risposta negativa, come operi, nella fase giurisdizionale, il recupero pieno delle garanzie a tutela del diritto fondamentale della persona invocata (nel necessario bilanciamento con gli altri diritti rilevanti). Occorrerà, infine, compiere una riflessione attenta anche sui rimedi esperibili, con particolare riferimento alla tutela cautelare che, a fronte di lesioni perpetrate via *web*, appare, in molti casi, l'unica forma di tutela idonea a garantire un rimedio effettivo.

Monica Velletti

Disciplina della prova nei procedimenti di diritto di famiglia

Sommario: 1. Premessa. – 2. Il diritto alla riservatezza dei dati personali. – 3. Fonti. – 4. Orientamenti dottrinali e giurisprudenziali in tema di c.d. prove illecite. – 4.1 Ragioni della scelta sub a): il diritto di difesa consente la produzione e l'acquisizione di documenti illecitamente acquisiti, senza eccezioni. – 4.2. Ragioni della scelta b): inutilizzabilità delle c.d. prove illecite. – 4.3 Ragioni della scelta c): tesi del bilanciamento di interessi. – 5. Le c.d. prove illecite nei procedimenti di famiglia. – 6. Analisi della giurisprudenza in materia di prove c.d. illecite nei procedimenti di diritto di famiglia. – 7. Conclusioni…..nei limiti del possibile.

1. Premessa

La tutela della *privacy* può confliggere con il diritto di difesa, con necessità di individuare criteri per dirimere il conflitto tra diritti fondamentali, esigenza particolarmente avvertita nei procedimenti in materia di diritto di famiglia. Per provare fatti e circostanze a sostegno delle domande, in molti casi, potrebbe essere necessario diffondere dati riservati della controparte o di terzi (si pensi a nomi o immagini di persone legate da relazioni sentimentali con il coniuge; a dati sensibili sull'uso di alcool o droga; a dati relativi alla situazione reddituale e patrimoniale della controparte; ad informazioni di carattere medico sanitario). Il diritto di azione e di difesa al quale viene riconosciuta tutela sia da norme costituzionali (art. 24 Cost.), sia da norme sovranazionali (art. 13 Convenzione europea dei diritti dell'uomo), può imporre la necessità di acquisire e diffondere, senza il consenso dell'interessato, dati personali sia della controparte sia di terzi, per far valere in giudizio un proprio diritto o per resistere all'altrui domanda. Occorre, pertanto, interrogarsi sui rapporti tra il diritto di azione e di difesa e il diritto alla riservatezza nel suo duplice significato: (C.M. Bianca)

– diritto alla protezione dei dati personali;
– diritto al rispetto della propria vita privata (*privacy*).

Il conflitto che può realizzarsi nei procedimenti di famiglia tra il diritto di azione e di difesa e il diritto alla protezione dei dati personali e al rispetto della vita privata può essere colto rappresentando concrete situazioni in cui il giudice

della famiglia e dei minori può essere chiamato a decidere. A questo fine invito ciascuno dei partecipanti all'incontro di studio a prendere posizione su alcuni casi che sto per rappresentare, tratti dalla mia esperienza professionale, quale giudice della Sezione famiglia del Tribunale di Roma.

Primo scenario: domanda di separazione, udienza presidenziale, due giovani coniugi, genitori di una bambina di due anni, compaiono davanti dal giudice delegato allo svolgimento di funzioni presidenziale per il tentativo di conciliazione. Dalla lettura degli atti risulta incontestato che la coppia è separata di fatto da qualche mese e che la moglie è rimasta a vivere con la minore nella casa coniugale in comproprietà tra le parti. Vi sono rilevanti divergenze quanto alle richieste sulla disciplina delle modalità di affidamento della minore, in quanto il marito chiede venga disposto affidamento condiviso con modalità di frequentazione genitori figlia sostanzialmente paritetiche, mentre la moglie, lamentando non meglio specificate condotte del padre potenzialmente pregiudizievoli per la minore, chiede l'affidamento super esclusivo a sé della figlia, con limiti finanche alla frequentazioni padre figlia da disporre alla presenza della madre o di persone di fiducia della stessa. All'udienza presidenziale viene disposto, alla presenza del difensore, l'interrogatorio libero del marito che riferisce di condotte della madre "ostative" in quanto, nell'ormai lungo periodo di separazione di fatto, in essere da oltre dieci mesi, la moglie non avrebbe mai consentito l'allontanamento dello stesso padre dalla casa familiare con la minore, pur consentendo regolari frequentazioni padre figlia (due o tre volte la settimana) nella casa familiare, alla presenza, seppur in altra stanza dell'immobile, della stessa madre, interrogato dal Presidente in merito alle ragioni di tale condotta, il padre dichiara di ritenere non fisiologico l'attaccamento materno alla minore, e di ravvisare nelle condotte della moglie comportamenti "ostativi" e "ritorsivi" rispetto alla scelta dello stesso di cessare la convivenza matrimoniale divenuta insostenibile a causa dei continui litigi, asseritamente provocati dal carattere controllante della moglie. Disposto l'interrogatorio libero della moglie la stessa pur confermando le resistenze a consentire una libera frequentazione tra il padre e la figlia minore, nega condotte "ostative" e più volte invitata a spiegare le ragioni delle resistenze a consentire la libera frequentazione padre figlia, afferma di nutrire timori a causa della tossicodipendenza del padre. Inviato il marito a rientrare nell'aula, nel contraddittorio di entrambe le parti, questi nega qualunque dipendenza, indicando anche in tali affermazioni, ritenute gravissime, indici dei profili caratteriali della moglie, capace di affermazioni false al solo fine di evitare il corretto esercizio della genitorialità paterna, con lesione del diritto della minore alla bigenitorialità. La moglie quindi estrae dalla borsa una pen drive affermando che nella stessa sono presenti riprese video, eseguite nell'abitazione delle parti, che ritrarrebbero il marito chiuso

nel bagno della casa familiare mentre assume droga per inalazione. Il marito nega di aver posto in essere le condotte asseritamente riprodotte nelle riprese, eccependone comunque l'illiceità in quanto acquisite in assenza di ogni consapevolezza in merito alla presenza di telecamere nell'abitazione, con conseguente violazione della diritto alla propria riservatezza. A fronte della richiesta del difensore della madre di acquisire i dati riportati nel supporto, e della opposizione del difensore della padre all'acquisizione, considerando che all'esito dell'udienza presidenziale devono essere assunti provvedimenti provvisori ed urgenti disciplinanti tra l'altro l'affidamento dei figli minori, da cui dipende l'assegnazione della casa familiare, immaginando di essere i giudici chiamati alla decisione, avreste o meno acquisito i dati illecitamente registrati?

Secondo scenario: domanda di separazione, udienza presidenziale, due coniugi di 45/50 anni, genitori di due figli adolescenti, compaiono davanti al giudice delegato a funzioni presidenziale per il tentativo di conciliazione. Dalla lettura degli atti risulta incontestato che la coppia è ancora convivente, il marito è artigiano e la moglie insegnante elementare, non vi sono sostanziali divergenze quanto alle modalità di affidamento condiviso dei figli che resteranno a vivere con la madre, nell'immobile in comproprietà tra le parti, con regolari frequentazioni paterne, mentre vi sono rilevanti divergenze in relazione alla quantificazione del contributo al mantenimento per la prole e per la ricorrente, in quanto la moglie rappresentando redditi del marito notevolmente superiori a quelli dichiarati, chiede l'imposizione a carico dello stesso di elevati contributi per il mantenimento dei figli e di un contributo per il di lei mantenimento. Il marito si oppone a queste richieste affermando di percepire i soli redditi indicati nelle dichiarazioni fiscali, offrendo pertanto un modesto contributo per il mantenimento dei soli figli. Nel corso dell'udienza presidenziale le parti confermano le rispettive posizioni, ma la moglie afferma che i rilevanti redditi frutto dell'attività "in nero" del marito sarebbero conservati nella cassaforte di casa, il marito nega tale circostanza, la moglie allora rappresenta di essere in possesso di riprese, memorizzate in una pen drive, che riprendono il marito che, ogni sera, al temine della giornata di lavoro apre la cassaforte e inserisce nella stessa denaro contante. La moglie chiede quindi di essere autorizzata a produrre il supporto per l'acquisizione delle riprese. Il marito nega di aver posto in essere le condotte asseritamente riprodotte nelle riprese, eccependo comunque l'illiceità della riproduzione audio video, in quanto acquisita in assenza di ogni consapevolezza della presenza di telecamere nell'abitazione, con conseguente violazione della riservatezza. A fronte della richiesta del difensore della moglie di acquisire i dati riportati nel supporto, e della opposizione del difensore del marito all'acquisizione, considerando che all'esito dell'udienza presidenziale devono essere assunti

provvedimenti provvisori ed urgenti che disciplinano tra l'altro le modalità di mantenimento dei figli, nella specie minori, e del coniuge che non abbia sufficienti risorse proprie, immaginando di essere i giudici chiamati alla decisione, avreste o meno acquisito i dati?

Terzo scenario: domanda di separazione, udienza presidenziale, due coniugi di 35/40 anni, genitori di due figli minori, compaiono davanti al giudice delegato a funzioni presidenziale per il tentativo di conciliazione. Dalla lettura degli atti risulta incontestato che la coppia è ancora convivente, vi sono divergenze quanto alle domande relative alle modalità di affidamento dei figli richiedendo la moglie, che ha formulato domanda di addebito, l'affidamento esclusivo dei figli a sé e il marito l'affidamento condiviso. La moglie nel corso dell'udienza motiva la richiesta di addebito della separazione al marito e di affidamento esclusivo dei figli a sé in ragione dell'esistenza di una relazione extraconiugale del marito con amica di famiglia, affermando di poter provare la circostanza con riprese eseguite nell'abitazione delle parti, che ritrarrebbero il marito in atteggiamenti intimi con l'altra donna. Il marito nega di aver posto in essere le condotte asseritamente riprodotte nelle riprese, eccependo comunque l'illiceità delle stesse in quanto assunte in assenza di ogni consapevolezza in merito alla presenza di telecamere nell'abitazione, con conseguente violazione del diritto alla riservatezza. A fronte della richiesta del difensore della moglie di acquisire i dati riportati nel supporto, e dell' opposizione del difensore del padre all'acquisizione, considerando che all'esito dell'udienza presidenziale devono essere assunti provvedimenti provvisori ed urgenti che disciplinano tra l'altro l'affidamento dei figli minori, immaginando di essere i giudici chiamati alla decisione, avreste o meno acquisito i dati?

Invito tutti i partecipanti a prendere posizione sui casi rappresentati per valutare al termine dell'intervento se esistono o meno soluzioni condivise.

2. Il diritto alla riservatezza dei dati personali

Il diritto alla riservatezza salvaguarda e tutela la sfera privata delle persone assicurando che ciascuno possa avere il controllo su tutte le informazioni e i dati riguardanti la propria vita personale. Ciascuno può impedire che informazioni riguardanti la propria sfera personale vengano diffuse in assenza di autorizzazione e ha diritto a non subire intromissioni nella propria sfera privata da parte di terzi. La tutela della *privacy* è un diritto assoluto. «*La tutela della privacy si è sempre più strutturata come un diritto di ogni persona al mantenimento del controllo sui propri dati, ovunque essi si trovino, così riflettendo la nuova situazione nella quale ogni persona cede continuamente, e nelle forme più diverse, dati che la riguardano….La sfera privata è un luogo di scambi, di condivisione di dati*

personali, di informazioni la cui circolazione non riguarda più soltanto quelle in uscita di cui altri possono appropriarsi o venire a conoscenza, ma interessa anche quelle in entrata, con le quali altri invadono quella sfera in forme sempre più massicce e indesiderate così la modificano continuamente» (S. Rodotà).

3. Fonti

La tutela della *privacy* e della riservatezza è disciplinata principalmente da fonti sovranazionali. L'art. 8 Convenzione Europea dei diritti dell'uomo, disciplina il "Diritto al rispetto della vita privata e familiare" prevedendo che "1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 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.". Manca, tuttavia, un'esplicita definizione normativa di «vita privata». Questa nozione è stata nel tempo riempita di contenuto dalle decisioni della Corte Europea dei diritti dell'Uomo che ha affermato come il diritto alla protezione della vita privata comprenda:

– il diritto di essere lasciato in pace (c.d. «*to let be alone*») inteso in senso verticale rispetto a possibili ingerenze dei pubblici poteri;
– il diritto a vedersi rappresentati in maniera fedele nel proprio contesto sociale (Cfr. Corte EDU 16 dicembre 1992, *Niemietz v. Germany*);
– il diritto alla c.d. autodeterminazione informativa con la possibilità di controllare le informazioni che circolano sulla propria persona (cfr. Corte EDU 29 aprile 2002, *Pretty v. UK*).

Anche nella Carta dei diritti fondamentali dell'Unione europea sono espressamente disciplinati i due aspetti del diritto alla riservatezza: l'art. 7 disciplina la *privacy*, il diritto di ogni individuo al rispetto della propria vita privata e familiare, sancendo che "Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni."; l'art. 8 disciplina la protezione dei dati di carattere personale, sancendo che "1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo 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 individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

La Carta Costituzionale e le norme di diritto interno, fino agli anni 90, non contenevano alcun espresso riferimento al diritto alla riservatezza. Il diritto alla riservatezza era nel diritto interno un diritto di creazione pretoria che trovava comunque copertura costituzionale negli artt. 13, 14 e 15 Cost..

Con l'adozione di fonti dell'Unione europea la materia ha avuto puntuale regolamentazione, ed è oggi disciplinata dal Regolamento Europeo (Reg. UE n. 679/2016, c.d. GDPR) entrato in vigore in data 25 maggio 2018. Il Reg. UE n. 679/2016 ha dettato una puntuale disciplina del trattamento dei dati personali fornendo, in primo luogo, una espressa definizione dei dati personali, qualificati come «qualunque informazione riguardante una persona fisica identificata o identificabile». Una speciale disciplina è prevista per particolari categorie di dati qualificati come «dati sensibili», categoria nella quale sono ricompresi i dati «che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, o filosofiche, l'appartenenza sindacale nonché i dati relativi alla vita sessuale e alla salute, ai dati genetici e ai dati biometrici». Di particolare rilevanza per il tema in esame è il considerando 4 del Reg. UE n. 679/2016, che fornisce le chiavi ermeneutiche per l'applicazione del regolamento, precisando che la tutela dei dati personali non è un diritto assoluto, ma è un diritto che si inserisce nel quadro delle fonti del diritto dell'Unione, con conseguente necessità per l'interprete di considerarne la funzione sociale, e di compiere un bilanciamento tra il diritto in esame e gli altri diritti fondamentali, parimenti riconosciuti dalle fonti euro-unitarie. Il considerando 4 del Reg. UE n. 679/2016 stabilisce che "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.". Deve essere sottolineato l'espresso richiamo al diritto di azione e difesa (il diritto a un ricorso effettivo e a un giudice imparziale), ulteriormente precisato nel considerando 52 Reg. UE n. 679/2016, nel quale è delineata la *ratio* delle deroghe al divieto di trattare particolari categorie di dati. Il considerando prevede che le deroghe possono essere previste, tra l'altro, per consentire di trattare dati personali «se necessario per accertare, esercitare o difendere un diritto che sia in sede giudiziale, amministrativa o stragiudiziale». Nel disciplinare il bilanciamento tra il diritto alla riservatezza e il diritto alla difesa, l'art. 9, Reg. UE n. 679/2016, attribuisce prevalenza a quest'ultimo

diritto, anche in presenza di dati sensibili. La norma, infatti, prevede alla lettera f), che è possibile trattare dati personali sensibili anche in assenza del consenso dell'interessato quando «il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali».

Il par. 4, dell'art. 9, Reg. UE n. 679/2016 ha consentito agli Stati Membri di prevedere ulteriori limitazioni per il trattamento dei dati sensibili. Il legislatore italiano utilizzando tale facoltà ha previsto all'art. 2 *septies* del Codice della Privacy che il Garante per la protezione dei dati personali possa disporre «misure di garanzia» per alcune categorie di dati, disponendo inoltre all'art. 2 *quater* che il Garante possa promuovere «regole deontologiche» con intese con ordini professionali.

L'art. 9, Reg. UE n. 679/2016, disciplina i soli dati sensibili e nel regolamento non è presente analoga disposizione con riferimento alle altre categorie di dati, ma ragioni sistematiche (non è possibile immaginare minore tutela per i dati sensibili rispetto agli altri dati) impongono di ritenere che sia possibile trattare dati personali non sensibili anche in assenza del consenso dell'interessato quando «il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali». La prevalenza del diritto di difesa rispetto al diritto di mantenere riservati i dati personali, dovrebbe sussistere per ogni categoria di dati e non solo per quelli sensibili.

La disposizione presente nell'art. 6, lett. f), Reg. UE n. 679/2016, qualifica come lecito il trattamento di tutti i dati personali quando «è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore». La disposizione fa ritenere che possa qualificarsi lecito il trattamento di ogni categoria di dati personali per agire o difendersi in giudizio.

Al fine di verificare la liceità del trattamento dei dati, anche sensibili, diffusi senza il consenso dell'interessato per agire o difendersi in giudizio, occorre pertanto dare contenuto alla nozione di "necessità del trattamento". Può ritenersi che il trattamento sia necessario solo qualora il dato personale della controparte o del terzo, portato in giudizio in assenza del consenso di colui al quale il dato si riferisce, attenga ad un fatto rilevante della controversia e non ad aspetti marginali. Non ogni esigenza difensiva può giustificare quindi l'uso di dati personali altrui ma solo quella che sia in grado di apportare contributo decisivo alla soluzione della controversia. Secondo un' interpretazione condivisa, il trattamento può ritenersi necessario quando sia

il solo modo per fornire la prova in giudizio. In merito la Corte EDU nella decisione 20 ottobre 2006, n. 7508/2002, *LL c. Francia*, ha affermato che per fornire la prova della colpa del marito in un giudizio di separazione non fosse necessario l'uso di documentazione medica del coniuge attestante la sussistenza di uno stato di alcolismo, quando la prova dell'allegazione poteva essere fornita con altri elementi che non prevedevano la divulgazioni di dati sensibili dell'interessato.

Ma come decidere qualora l'uso di dati personali altrui possa essere non l'unico modo ma il modo più rapido ed efficace per assumere decisioni in tema di diritti fondamentali, quali quelli che vengono in esame nei procedimenti in materia di diritti dei minori e di famiglia?

4. Orientamenti dottrinali e giurisprudenziali in tema di c.d. prove illecite

Compiuti questi brevi cenni preliminari, in merito al rapporto tra diritto alla difesa e diritto alla *privacy* ed alla tutela dei dati personali, secondo le nuove disposizioni contenute nel Reg. UE n. 679/2016, prima di analizzare nello specifico la disciplina della prova nei procedimenti di famiglia, appare opportuno richiamare gli orientamenti dottrinali e giurisprudenziali in merito alla c.d. "prove illecite", in quanto in molti casi le prove precostituite che vengono prodotte nel corso del giudizio in violazione del diritto della riservatezza altrui sono acquisite con condotte poste in violazione di norme penali (si pensi all'acquisizione di corrispondenza, di immagini, di conversazioni telefoniche, di dati estrapolati da computer personali, senza il consenso del titolare dei dati).

Il dibattito dottrinale e giurisprudenziale sul tema delle c.d. «prove illecite», cioè delle prove acquisite in violazione di norme che tutelano diritti fondamentali – quali la corrispondenza, l'immagine, la riservatezza, i dati personali– è molto risalente.

«*A prima vista verrebbe voglia di dire: il giudice cerca la verità e quando una prova gli serve per fargliela conoscere, se ne deve giovare; se chi gliela ha fornita ha offeso, per procurarsela, il diritto altrui, ne risponderà; intanto, però, il servigio alla giustizia è reso*» Carnelutti, (*Illecita produzione di documenti*, in *Riv. dir. proc.,* 1935, 63), l'Autore pur partendo da tale affermazione concludeva affermano che doveva ritenersi impossibile che chi avesse commesso un delitto potesse giovarsi a fini probatori di una condotta *contra legem*.

Il tema è stato affrontato nella dottrina e nella giurisprudenza in numerosi settori (diritto del lavoro, nelle cause commerciali) ma è indubbiamente l'ambito delle controversie in materia familiare quello nel quale con maggiore evidenza emerge il potenziale conflitto tra l'esercizio del diritto di difesa della parte che in-

tende produrre in giudizio la prova ottenuta in violazione di norme che tutelano altri diritti fondamentali (corrispondenza, *privacy*, etc) e le norme che tutelano tali diritti.

Per l'esatta ricostruzione della tematica occorre distinguere tra:

– modalità di acquisizione della prova;
– risultato della acquisizione, il documento (inteso in senso lato come scritto, riproduzione fotografica, telematica, registrazione) frutto dell'illecita attività di acquisizione.

La condotta che può porsi in potenziale contrasto con le norme di pari rango, a volte sanzionata in disposizioni di natura penale, attiene al primo dei due aspetti indicati, riguardando infatti la condotta di «ricerca» della prova. Si pensi alla violazione della corrispondenza per acquisire missive riservate, ovvero alla condotta che integri il delitto di interferenza illecita nella vita privata, per acquisire senza il consenso della parte, informazioni sulla vita privata della stessa. La condotta di colui che per acquisire la prova viola una norma penale potrà essere oggetto di accertamento e di sanzione penale. Mentre il documento, una volta acquisito seppure illecitamente, potrebbe essere considerato una prova precostituita e come tale suscettibile di essere introdotto nel processo.

La soluzione non è pacifica né univoca, soprattutto nei casi in cui il documento contenga dati sensibili.

Infatti, quanto alla possibilità di avvalersi in giudizio del documento contenente dati personali illecitamente acquisiti le opzioni ermeneutiche che si contrappongono sono essenzialmente tre:

a) il diritto di difesa consentirebbe la produzione e l'acquisizione di documenti illecitamente acquisiti, senza eccezioni;
b) i documenti illegittimamente acquisiti sarebbero al pari di quanto accade nel processo penale inutilizzabili;
c) non sarebbe possibile fornire una risposta univoca per ogni fattispecie essendo necessario compiere un bilanciamento tra i contrapposti diritti «caso per caso».

4.1 Ragioni della scelta sub a): il diritto di difesa consente la produzione e l'acquisizione di documenti illecitamente acquisiti, senza eccezioni

A fondamento di tale opzione ermeneutica vi è la constatazione che nel codice di procedura civile non è prevista un'espressa sanzione della inutilizzabilità delle prove costituite acquisite in modo illecito (al contrario di quanto previsto nell'art. 191 c.p.p.). Diversamente da quanto previsto nel processo penale, il disposto dell'art. 115 comma 1 c.p.c., imporrebbe al giudice di valutare tutte le prove prodotte dalle parti nel rispetto delle regole proprie del codice di procedu-

ra civile (si pensi in particolare al rispetto dei termini *ex* art. 183 c.p.c.). «*Le prove precostituite, quali i documenti, entrano nel giudizio attraverso la produzione e nella decisione in virtù di un'operazione di semplice logica giuridica, essendo tali attività contestabili solo se svolte in contrasto con le regole, rispettivamente, processuali o di giudizio, che vi presiedono, senza che abbia rilievo una valutazione in termini di utilizzabilità, categoria propria del rito penale ed ignota al processo civile*» (Cass. 25 marzo 2013, n. 7466; Cass. 14 novembre 2012, n. 19870). In questo senso sembra orientata la prevalente giurisprudenza di merito (Trib. Milano, impresa 27 luglio 2016 sulla utilizzabilità di e.mail frutto di accesso abusivo; Trib. Torino 8 maggio 2013).

4.2. Ragioni della scelta b): inutilizzabilità delle c.d. prove illecite

L'acquisizione di prove illecite si porrebbe in insanabile contrasto con i diritti fondamentali della persona tutelati dalla Costituzione, con conseguente "inutilizzabilità" delle stesse. In tal senso si è espressa la Suprema Corte (Cass. 8 novembre 2016, n. 22677) in tema di affidamento dei figli in giudizio di separazione, ritenendo corretta la scelta del giudice di merito che aveva negato la possibilità di acquisire file audio sottratti alla controparte, in assenza di consenso.

In particolare, le prove acquisite in violazione delle liberà personali si porrebbero in contrato con l'art. 13, comma 3, Cost.; le prove acquisite in violazione del domicilio si porrebbero in contrato con l'art. 14, comma 1, Cost.; le prove acquisite in violazione alle «libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione» si porrebbero in contrato con l'art. 15, comma 1, Cost..

Secondo i sostenitori di questa scelta interpretativa, sarebbe la stessa Costituzione a stabilire che la limitazione di diritti fondamentali, quali quelli richiamati, possa avvenire soltanto per atto motivato dell'Autorità giudiziaria con le garanzie stabilite dalla legge. Poiché è la Costituzione a stabilire che la limitazione di tali libertà fondamentali possa avvenire esclusivamente per atto motivato dell'Autorità giudiziaria con le garanzie stabilite dalla legge, l'acquisizione di documenti in violazione di tali diritti renderebbe la prova illecita inutilizzabile.

Inoltre, il diritto alla riservatezza, troverebbe tutela nelle fonti sovranazionali:

- art. 8, commi 1 e 2, della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali;
- art. 2 della Dichiarazione universale dei diritti dell'uomo.

La presenza di limiti invalicabili, cristallizzati in norme di rango sovranazionale, non permetterebbero al giudice di acquisire nel corso del processo civile, documenti entrati nella disponibilità della parte, che intenda produrli, in violazione delle richiamate disposizioni poste a tutela di diritti fondamentali.

4.3 Ragioni della scelta c): tesi del bilanciamento di interessi

In applicazione di tale opzione, per escludere l'ammissibilità di una prova acquisita con modalità illecite, sarebbe necessaria la sussistenza di una norma processuale che ne sancisca espressamente la nullità, essendo preclusa al giudice la valutazione di ammissibilità di prove precostituite in giudizio. In mancanza di sanzione espressa la violazione di norme, anche di rilevanza penale che sanzionino la condotta illecita di acquisizione della prova, non sarebbe sufficiente a far ritenere inammissibile l'acquisizione del documento (inteso in senso lato) frutto dell'attività illecita. Per decidere in merito alla acquisizione sarebbe, invece, necessario compiere un bilanciamento tra i diritti che chi richiede l'acquisizione del documento intende difendere e i diritti e gli interessi fondamentali che il soggetto nei confronti dei quali la c.d. prova illecita è prodotta assume essere stati lesi.

Il bilanciamento deve essere operato tra: il diritto alla difesa e alla prova da un lato e il diritto alla riservatezza e alla protezione dei dati personali, dall'altro.

In merito la Suprema Corte ha evidenziato l'esistenza una "gerarchia mobile" nel bilanciamento dei contrapposti interessi "*da intendersi non come rigida e fissa subordinazione di uno degli interessi all'altro, ma come concreta individuazione da parte del giudice dell'interesse da privilegiare tra quelli antagonistici, a seguito di una ponderata valutazione della specifica situazione sostanziale dedotta in giudizio con conseguente bilanciamento tra gli stessi, capace di evitare che la piena tutela di un interesse possa tradursi nella limitazione di quello contrapposto tanto da vanificarne o ridurne il valore contenutistico…..*" (Cass., 5 agosto 2010, n. 18279, in tema di licenziamento), precisando che "*l'operazione di bilanciamento può condurre ad un arretramento di tutela dei dati personali tutte le volte in cui nel conflitto di interessi il grado di lesione della dignità dell'interessato sia di ridotta portata rispetto a quella che subirebbe il diritto antagonista, non potendo consentirsi all'interessato di trincerarsi dietro l'astratta qualificazione del suo diritto si da limitare in maniera rilevante il diritto di difesa della controparte.*" (Cass., 5 agosto 2010, n. 18279, cit.; in senso conforme Cass. 30.6.2009 n. 15327; Cass. 7.7.2008 n. 18584).

5. Le c.d. prove illecite nei procedimenti di famiglia

Nell'ambito dei procedimenti di diritto di famiglia il bilanciamento di interessi potrebbe far propendere per l'ammissibilità di prove illecitamente acquisite in ogni caso in cui la prova sia posta a fondamento di domande attinenti diritti fondamentali di rango elevato.

Per individuare una linea, non arbitraria, per distinguere tra diritti fondamentali di rango elevato e diritti non appartamenti a questa categoria, potrebbe essere utilizzato un preciso parametro normativo, presente nella disciplina della

materia, considerando come criterio determinante la scelta del legislatore di riconoscere al giudice poteri officiosi. Se, infatti, il giudice può disporre al di fuori del limiti della domanda (come accade, per esempio, nei procedimenti in materia di minori) ovvero può attivare poteri istruttori d'ufficio (come accade in materia di disciplina delle modalità di mantenimento della prole ma anche del coniuge debole), significa che l'ordinamento riconosce a tali diritti rango sopraelevato, imponendo al giudice di garantire le parti deboli del rapporto, attribuendo all'organo giudicante un ruolo attivo nel processo. Ferma la terzietà del giudice, l'oggettiva valutazione compiuta *ex ante* dal legislatore della presenza di parti meritevoli di una tutela rafforzata, ha portato all'introduzione nell'ordinamento di norme che attribuiscono al giudice proprio il ruolo di riequilibrio delle posizioni delle parti all'interno della dinamica processuale, che potrebbe essere compromessa in ragione della fragilità di una delle parti, in mancanza di ricostituzione della c.d. "parità delle armi".

Tali poteri officiosi sono massimi, inerendo non solo gli aspetti della prova ma anche la possibilità di incidere sulla stessa domanda, nei procedimenti che hanno ad oggetto diritti relativi ai minori. Il giudice della crisi familiare può, infatti, adottare provvedimenti diversi e contrari rispetto a quelli richiesti dalle parti non solo per i provvedimenti aventi ad oggetto domande relative all'affidamento della prole (*ex multis*: Cass. 31 marzo 2014, n. 7477; Cass. 10 maggio 2013, n. 11218; Cass. 20 giugno 2012, n. 10174 e Corte Cost. 14 luglio 1986, n. 185), ma anche per quelli che hanno ad oggetto domande per la disciplina delle modalità di mantenimento dei figli minori (Cass. 30 dicembre 2011, n. 30196; Cass. 18 febbraio 2009, n. 3908; Cass. 30 dicembre 2011, n. 30196). Il legislatore ha attribuito al giudice procedente il potere di emettere pronunce anche al di fuori dei limiti della domanda (ferma la necessità di instaurare sul punto in contraddittorio), ovvero di assumere delle prove anche al di fuori delle richieste delle parti; poteri officiosi che ovviamente possono essere attivati solo a favore del minore, nel perseguimento del suo superiore interesse.

Il fondamento normativo di poteri dispositivi del giudice in materia di minori si rinviene nell'art. 337-*ter* c.c., nel quale è previsto che il giudice, nei procedimenti di separazione, divorzio, modifica delle condizioni di separazione e divorzio, disciplina delle modalità di affidamento e mantenimento dei figli nati fuori del matrimonio (e negli altri procedimenti di cui all'art. 337-bis c.c.), possa adottare «ogni altro provvedimento relativo alla prole». Questo principio è applicabile in tutte le tipologie di provvedimenti emanati nel corso del giudizio (ordinanza presidenziale, eventuale decreto della Corte d'Appello che riformi o modifichi l'ordinanza presidenziale, provvedimenti provvisori del giudice istruttore, sentenza definitiva), provvedimenti provvisori o definitivi emessi all'esito di procedimento camerale. Per l'esercizio dei poteri officiosi del giudice, a tutela

dei minori, non ci sono vincoli temporali o sistematici, sono poteri riconosciuti dall'ordinamento indipendentemente dalla natura decisoria o soltanto istruttoria del provvedimento, ovvero dal suo grado di stabilità (provvedimenti definitivi o provvisori).

Il fondamento di poteri istruttori del giudice per l'adozione di provvedimenti a tutela della prole si rinviene nell'art. 337-*octies* c.c., nel quale è previsto che «prima dell'emanazione, anche in via provvisoria, dei provvedimenti di cui all'articolo 337-*ter*, il giudice può assumere, ad istanza di parte o d'ufficio, mezzi di prova».

Se il giudice nell'adottare provvedimenti relativi ai minori non è vincolato al principio della domanda ed ha poteri istruttori d'ufficio, deve ritenersi che *ratio* di tali disposizioni sia da ravvisare nell'attribuzione in capo al giudice di poteri finalizzati alla esatta ricostruzione dei fatti e della situazione familiare, con conseguente necessità di ammettere prove, anche se illecitamente acquisite in violazione di norme sia penali sia a tutela della *privacy*, qualora necessarie per accertare fatti decisivi per l'adozione di provvedimenti a tutela dei figli.

Appare che identiche conclusioni potrebbero essere formulate in tutti quei casi in cui il legislatore ha attribuito al giudice poteri d'ufficio nell'ambito dei procedimenti in materia di famiglia, pur mantenendo il vincolo della domanda. Si pensi per esempio alle norme che hanno attribuito al giudice il potere di disporre indagini di polizia tributaria per l'accertamento dei redditi di uno dei coniugi ai fini dell'accertamento del diritto del c.d. coniuge debole a ricevere assegno di mantenimento ovvero assegno divorzile, ovvero per determinare il contributo per il mantenimento dei figli maggiorenni non economicamente autosufficienti. In queste ipotesi, potendo il giudice attivare d'ufficio poteri istruttori, deve ritenersi che sia possibile l'acquisizione di c.d. prove illecite, che tendono a conseguire il medesimo risultato. Rappresenterebbe, infatti, un inutile dispendio di energie processuali ritenere inammissibile, per esempio, il deposito di estratti di conti correnti, acquisiti illecitamente del coniuge debole violando il diritto alla segretezza della corrispondenza dell'altro coniuge (si pensi alla acquisizione non autorizzata della corrispondenza dell'istituto bancario recapitata nella casa familiare), in presenza di poteri normativamente attribuiti al giudice della famiglia che gli consentirebbero di rivolgere ordine diretto agli istituti di credito per ottenere la medesima documentazione, ovvero di disporre indagini di Polizia tributaria al medesimo fine.

Al contrario, in assenza di poteri officiosi normativamente attribuiti al giudice, e pertanto in mancanza di parametri che permettono di far ritenere nel giudizio di bilanciamento prevalente il diritto di azione in presenza di determinati interessi (come quello alla tutela del minore, ovvero alla tutela "economica" del coniuge debole o del figlio maggiorenne non autosufficiente) rispetto al diritto alla

riservatezza o alla *privacy*, non sarebbe possibile disporre l'acquisizione delle c.d. prove illecite.

Quanto esposto rappresenta l'applicazione ai procedimenti di famiglia di una delle opzioni ermeneutiche possibili, e proprio la mancanza di orientamenti univoci fa ritenere opportuno riportare parte della giurisprudenza di merito e legittimità per sottolineare le diverse posizioni. In una materia tanto dibattuta richiamare la giurisprudenza, anche e soprattutto di merito, può consentire a ciascuno di approfondire le argomentazioni contenute nei diversi provvedimenti, per maturare il proprio convincimento, nell'attesa di un sempre auspicato intervento normativo che detti disposizioni di univoca lettura.

6. Analisi della giurisprudenza in materia di prove c.d. illecite nei procedimenti di diritto di famiglia

Si riporta parte della giurisprudenza di merito e legittimità per sottolineare le diverse posizioni cercando di distinguere le pronunce in considerazione delle diverse domande oggetto di decisione.

Procedimenti aventi ad oggetto domanda di affidamento minore: nel corso di un giudizio per la disciplina delle modalità di affidamento di figlio minore nato da genitori non coniugati è stata ammessa l'acquisizione di immagini registrate con telecamere collocate in casa, senza il consenso del genitore ripreso nelle immagini, per provare l'uso di sostanze stupefacenti da parte dello stesso (Trib. Roma, decr. 20 gennaio 2017). Si riporta parte della motivazione del provvedimento citato: «*Nel processo civile non è applicabile la sanzione della nullità di prove acquisite con modalità ritenute non lecite poiché manca una norma che la preveda espressamente, al contrario di quanto previsto nel processo penale ex art. 191 c.p.p. È compito dunque del Giudice bilanciare gli interessi che si contrappongono, individuando la soluzione più corretta nell'esclusivo interesse del minore (Nel caso di specie, l'oggetto della prova riguardava condotte del padre potenzialmente pregiudizievoli per la figlia minore, ambito nel quale i poteri di ufficio riconosciuti al giudice procedente superano i limiti del processo dispositivo, permettendo l'acquisizione di ogni elemento idoneo per valutare correttamente la situazione del minore e scegliere la soluzione migliore nel suo esclusivo interesse*)».

Procedimenti aventi ad oggetto domanda di disconoscimento di paternità: è stato ritenuto sussistente il divieto di acquisizione illecita di campione biologico per esame del DNA (Cass., 13 settembre 2013, n. 21014) "*Il trattamento di dati genetici di carattere non sanitario, finalizzato ad estrarre informazioni relativa al DNA per orientare la scelta verso un'azione di disconoscimento di paternità, con l'accertamento preventivo della consanguineità mediante un test predittivo,*

non è legittimo sulla base della sola Autorizzazione generale del Garante n. 2 del 2002, ma richiede il previo consenso dell'interessato, dovendosi inoltre rilevare, al riguardo, una continuità di regime giuridico, nel trattamento dei dati genetici, tra la fase anteriore e quella successiva all'emanazione dell'apposita Autorizzazione del 22 febbraio 2007, prescritta dall'art. 90 del d.lgs. 30 giugno 2003, n. 196. (Nella specie, la S.C. ha enunciato il principio con riferimento ad una controversia riguardante il trattamento di dati genetici, ottenuti mediante prelievo di mozziconi di sigaretta da parte di una agenzia investigativa e sottoposti, senza il consenso del titolare, al prelievo di campioni biologici ed accertamento del DNA).

Procedimenti di separazione giudiziale aventi ad oggetto domande di addebito: È stata ritenuta lecita la produzione di SMS acquisiti da un telefono lasciato nella casa familiare qualora i messaggi fossero visibili (Trib. Roma, 17 maggio 2017) «*In tema di separazione giudiziale dei coniugi, la prova dell'adulterio (nella specie, del marito) ben può fondarsi su messaggi (Sms) estratti dal telefono cellulare dell'uomo, di cui la moglie è entrata in possesso, essendo recessivo, rispetto al diritto di difesa in giudizio, quello alla inviolabilità della corrispondenza*.».

È stata ritenuta lecita la produzione di dati inseriti volontariamente da un'altra persona nella pagina personale del social network (nella specie foto tratte da social network) (Trib. Santa Maria Capua Vetere, 13 giugno 2013).

È stata ritenuta l' «inutilizzabilità» dei dati contenuti nell'hard disk del marito prelevato dall'altro coniuge e contenente immagini ed informazioni sulle abitudini sessuali del marito (Trib. Larino, 9 agosto 2017).

È stato ritenuto ammissibile il deposito, come prova a fondamento della domanda di addebito della separazione, delle riprese video realizzate mediante una telecamera posizionata nell'abitazione all'insaputa dell'altro coniuge (Trib. Roma, 20 gennaio 2017).

È stato ritenuto ammissibile utilizzare relazioni investigative corredate da foto, nonché i tabulati telefonici, per provare la domanda di addebito (Cass. 23 maggio 2014 n. 11516) "*Sotto il primo profilo, la ricorrente si duole del fatto che la corte territoriale abbia fondato il proprio convincimento su di una relazione investigativa redatta da persona incaricata dal marito, sulle fotografie in essa contenute e su alcuni tabulati telefonici dal medesimo prodotti. Quanto all'utilizzo della relazione investigativa redatta da tecnico incaricato da una delle parti del giudizio, la liceità di tale condotta è stata da questa Corte reiteratamente affermata: così, nell'ambito dei rapporti di lavoro, ove è consentito al datore di incaricare un'agenzia investigativa al fine di verificare condotte illecite da parte dei dipendenti (fra le altre, Cass. 22 novembre 2012, n. 20613; Cass. 8 giugno 2011, n. 12489; Cass. 14 febbraio 2011, n. 3590; Cass. 22 dicembre 2009, n. 26991,*

quest'ultima discorrendo della facoltà del datore di ricorrere ai mezzi necessari ad assicurare la stessa sopravvivenza dell'impresa contro attività fraudolente; Cass. 9 luglio 2008, n. 18821; Cass. 7 giugno 2003 n. 9167)".

In merito al potenziale conflitto tra il diritto alla *privacy* e il diritto di difesa si è pronunciata la Corte EDU, ritenendo contrario al diritto al rispetto della vita privata di cui all'art. 8 CEDU il pedinamento di un soggetto al fine di realizzare una relazione investigativa, nel caso di specie protrattosi per oltre 20 giorni, ritenendo tale intrusione non proporzionata (Corte EDU 18 ottobre 2016, *Vukota-Bojic c. Svizzera*)

7. Conclusioni… nei limiti del possibile

Prima di cercare di trarre le conclusioni dalle riflessioni svolte, appare opportuno analizzare le risposte dei partecipanti all'incontro di studio, inserite nella chat, sulle domande formulate all'inizio dell'intervento. La complessità della materia si coglie dall'assenza di unanimità nelle risposte. Per il primo degli scenari descritti, emerge una netta prevalenza di coloro che avrebbero ammesso l'acquisizione delle immagini illecitamente carpite per dimostrare lo stato di tossicodipendenza del padre della minore; per il secondo scenario vi è una sostanziale divisione tra coloro che avrebbero ammesso il deposito di immagini che riproducevano il marito mentre depositava nella cassaforte denaro in contante, e coloro che avrebbero rigettato la richiesta; per il terzo scenario vi è prevalenza di coloro che non avrebbero ammesso il deposito di immagini illecitamente carpire riproducenti la relazione extraconiugale del marito.

Come anticipato i tre casi sono tratti dalla mia personale esperienza giudiziaria, posso quindi indicare come ho effettivamente deciso: nel primo caso ho, senza dubbi, ammesso il deposito delle immagini dalle quali si desumeva l'uso di sostanze stupefacenti da parte del padre della minore. Era per me troppo urgente sapere immediatamente quale fosse la reale situazione, in quanto se è pur vero che il giudice, per accertare la tossicodipendenza, avrebbe potuto disporre analisi a carico del padre, tuttavia in primo luogo la parte avrebbe potuto rifiutare di sottoposi alle stesse, e comunque ogni indagine (da demandare necessariamente a strutture pubbliche) anche in presenza del consenso paterno avrebbe imposto tempi di attesa, incompatibili con la disciplina delle modalità di affidamento di un minore. Nel secondo caso, ho parimenti ammesso il deposito delle immagini, in quanto era necessario assumere i provvedimenti provvisori, e con gli ordinari strumenti probatori (presumibilmente le sole prove testimoniali) avrei dovuto attendere molto tempo, per avere risposte urgenti, al fine di determinare congrui assegni di mantenimento per la prole e per il coniuge debole. Nel terzo caso, non ho avuto dubbi a rigettare l'ammissione della prova, non rilevando l'even-

tuale presenza di violazioni del vincolo di fedeltà coniugale da parte del marito né ai fini delle modalità di affidamento dei figli (non essendo neppure allegate condotte pregiudizievoli poste in essere dalla compagna del padre), né ai fini della determinazione degli obblighi di mantenimento non avendo il marito formulato domanda di contributo economico.

Proprio l'esito dell'esperimento oggi compiuto, per i cui esiti ringrazio tutti coloro che ne hanno preso parte, allo stato attuale della giurisprudenza non sembra possibile dare una risposta univoca alla domanda relativa alla possibilità di porre a fondamento di un giudizio in materia familiare una prova che violi il diritto della altrui riservatezza.

Dai contenuti del Reg. UE n. 679/2016 (artt. 6 e 9) il diritto alla *privacy* appare recessivo rispetto alla tutela del diritto di difesa, ogni qual volta sussista il requisito della «necessità». È comunque necessario verificare oltre ai contenuti della prova che contenga dati personali in assenza del consenso dell'interessato, anche le modalità di acquisizione, perché se le modalità di acquisizione sono illecite la risposta in merito alla sua acquisizione/utilizzabilità è, come sopra detto, diversificata.

L'opzione ermeneutica che appare preferibile, ad avviso della scrivente, è quella del bilanciamento degli interessi che consente di sacrificare il diritto alla *privacy*, e finanche il diritto al rispetto delle norme di condotta che impongono il divieto di acquisire prove in violazione di diritti di rango costituzionale solo quando in giudizio vi siano da tutelare diritti di pari grado, in particolare quelli per i quali lo stesso legislatore concede al giudice procedente ampi poteri d'ufficio (nel diritto di famiglia si pensi alla tutela dei diritti dei minori, ma anche alla determinazione del contributo economico per prole, per il coniuge e per l'ex coniuge).

Quanto a prove tendenti a dimostrare la violazione di doveri coniugali, occorre distinguere, poiché qualora la prova che rechi violazione della riservatezza del coniuge (anche se acquisita in violazione di norme penali) serva a dimostrare agiti di violenza domestica, il bilanciamento di interessi e i poteri del giudice civile in materia (per esempio per emissione di ordini di protezione) fanno affermare alla scrivente l'opportunità dell'acquisizione della prova illecita, in nome del più volte richiamato bilanciamento degli interessi

In merito proprio la sentenza della Suprema Corte da ultimo citata n. 21014/2013, è ulteriore spunto per sostenere l'opportunità di un bilanciamento mobile degli interessi coinvolti. Nel caso di illecito prelievo di campione biologico la mancata ammissione della prova illecitamente acquisita, non provoca effetti negativi, in quanto all'accertamento della verità processuale si può comunque pervenire, in considerazione della consolidata giurisprudenza per la quale il mancato consenso della parte a sottoporsi nel contesto giudiziario ad

accertamento del DNA é argomento di prova sufficiente per l'accertamento della filiazione ovvero per il rigetto della domanda di disconoscimento (per tutte Cass. 5 giugno 2018, n. 14458).

In tutte le altre ipotesi in cui sia richiesta la tutela di diritti di rango costituzionale, la mancata acquisizione della prova illecita potrebbe pregiudicare la tutela di tali diritti. Dalla mancata acquisizione potrebbe derivare, infatti, l'impossibilità di raggiungere *aliund*e analoga prova (si pensi a prove illecitamente acquisite che dimostrino redditi c.d. «in nero»; ovvero a riprese video non autorizzate che documentino agiti di violenza domestica, elementi che occorre acquisire, ai sensi dell'art. 31 della Convenzione di Istanbul, oltre che per la tutela della vittima, anche al fine di disciplinare i diritti di affidamento e di visita dei figli).

Un approccio «rigido» che escludesse l'ammissione di tali prove illecite, in nome la loro «inutilizzabilità», potrebbe pregiudicare un'efficace tutela di diritti di rango costituzionale, qualora il giudice non possa acquisire *aliunde* la prova, mancando nel nostro ordinamento un principio che colleghi alla mancata collaborazione della parte la piena prova dei fatti allegati dall'altra (secondo quanto invece affermato in caso di mancata sottoposizione al test del DNA).

Federica Fiorillo[1]

Minori. Aspetti specifici della protezione dati[2]

Sommario: 1. Premessa. – 2. La tutela dei dati personali dei minori prima del Regolamento generale sulla protezione dei dati. – 2.1. Panoramica internazionale. – 2.2. Prospettiva di diritto interno. – 3. Il GDPR: la tutela dell'azione dei minori nel mondo digitale. – 3.1. Art. 8 GDPR: il consenso del minore in relazione ai servizi forniti dalle società dell'informazione – 3.2. Art. 17 GDPR: diritto all'oblio ed alla cancellazione dei dati personali dei minori – 4. Limiti della disciplina del GDPR a tutela dei minori e spunti conclusivi.

1. Premessa

Il tema della tutela dei dati personali dei minori non è nuovo, il Regolamento generale sulla protezione dei dati o GDPR (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) ha tuttavia introdotto alcune disposizioni innovative dirette in particolare a garantire la tutela dei dati personali dei minori con riferimento alla loro azione nel mondo digitale e dunque nella rete.

Secondo recenti studi un utente su tre della rete internet è minore[3] e si può pertanto intuire la fondamentale importanza di tali disposizioni.

Lo scopo della presente relazione è quello di fornire una breve panoramica delle normative antecedenti l'entrata in vigore del GDPR e del Codice in materia

---

[1] Le opinioni contenute in questo contributo sono espresse dall'autrice a titolo esclusivamentepersonale e non impegnano in alcun modo l'amministrazione di appartenenza.

[2] Trascrizione della presentazione effettuata nell'ambito del corso "Trattamento dei dati personali in ambito giudiziario" (P21003).

[3] Tale affermazione è stata svolta in seno alla recente presentazione, in data 10 dicembre 2020, da parte del Comitato sui diritti dei bambini del Consiglio d'Europa del Manuale per i responsabili politici sui diritti del bambino nell'ambiente digitale https://www.coe.int/en/web/children/home/-/asset_publisher/m06SMMbKyjRF/content/-all-on-board-all-online-launch-of-the-new-council-of-europe-handbook-for-policy-makers-on-the-rights-of-the-child-in-the-digital-environment?inheritRedirect=true&redirect=%2Fen%2Fweb%2Fchildren%2Fhome

di protezione dei dati personali come integrato con le modifiche introdotte dal decreto legislativo 10 agosto 2018, n. 101, attuativo delle disposizioni del Regolamento, accennando ad alcune questioni che si possono definire "tradizionali" in tema tutela dei dati personali dei minori, per poi soffermare l'attenzione sulle specifiche disposizioni del GDPR, concludendo infine con qualche breve riflessione su possibili sviluppi futuri.

Non si tratta di nozioni teoriche fini a sé stesse, ma di alcuni spunti di riflessione sulle tematiche suscettibili di venir in rilievo e sulla normativa applicabile nell'ambito di una causa. Limitando l'attenzione ad una prospettiva civilistica, si possono infatti citare alcuni esempi di controversie in cui possono porsi questioni di tutela dei dati personali dei minori.

Vanno citate innanzitutto le cause di famiglia ed in particolare le controversie *ex* art. 709 *ter* Codice Procedura Civile sull'esercizio della responsabilità genitoriale: esempi tipici sono costituiti dalle liti tra genitori aventi ad oggetto la pubblicazione delle fotografie e delle immagini dei figli minori sui *social networks*; si può pensare anche a liti aventi ad oggetto la stessa iscrizione di un minore ad un *social network*. Ancora, vengono in rilevo ricorsi cautelari d'urgenza aventi ad oggetto la rimozione di immagini o la cancellazione di dati e l'inibizione della ripetizione di determinati comportamenti lesivi. Si può infine, in via non esaustiva, pensare a cause ordinarie dirette all'accertamento del comportamento lesivo e della lesione, a far cessare il comportamento e ad ottenere il risarcimento del danno; a cause aventi ad oggetto la cancellazione di dati ed immagini; ancora, a cause dirette ad ottenere l'annullamento di contratti stipulati on line dal minore ed in particolare dell'atto con cui si è acquisito il consenso del minore rispetto al trattamento dei propri dati personali e di ogni conseguente trattamento dei dati stessi. Gli attori in tali cause saranno tipicamente rappresentanti del minore esercenti la responsabilità genitoriale o il minore stesso una volta raggiunta la maggiore età, eventualmente anche nei confronti degli stessi genitori. Convenuti potranno essere, in via esemplificativa, l'altro genitore; il soggetto titolare del trattamento di dati personali dei minori (ad esempio l'istituto scolastico); la società dell'informazione che abbia fornito il servizio di cui ha usufruito il minore ai sensi dell'art. 4 GDPR.

2. La tutela dei dati personali dei minori prima del Regolamento generale sulla protezione dei dati.

Per quanto concerne il tema della tutela dei dati personali dei minori prima del Regolamento generale sulla protezione dei dati, e dunque, semplificando, prima della disciplina specifica della azione dei minori nel mondo digitale, vanno citati innanzitutto i principi sanciti da Convenzioni e normative internazionali, per poi passare ad approfondire alcuni aspetti specifici regolati dal diritto interno.

2.1. Panoramica internazionale.

Sul piano internazionale vengono in rilievo innanzitutto le convenzioni internazionali e le disposizioni del diritto europeo che hanno affermato in maniera generale il diritto di ogni individuo, e dunque del minore, al rispetto ed alla protezione della propria vita privata e familiare e di tutto ciò che la costituisce, compresa la non divulgazione di notizie e dati attinenti alla stessa.

Vanno citati in tal senso l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e e gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (Cd. Carta di Nizza), nonché l'art. 16 del Trattato sul Funzionamento dell'Unione europea che ha posto le basi per l'emanazione del Regolamento generale sulla protezione dei dati.

Convenzione Europea per la salvaguardia dei diritti dell'Uomo e delle libertà fondamentali

Art. 8 Diritto al rispetto della vita privata e familiare

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

Carta dei diritti fondamentali dell'Unione europea

Art. 7 Rispetto della vita privata e della vita familiare

1. *Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni.*
2. *Deve farsi inoltre riferimento alle disposizioni specificamente rivolte alla tutela dei dati personali, quali l'art. 8 della Carta di Nizza e l'art. 16 del Trattato sul Funzionamento dell'Unione europea.*

Carta dei diritti fondamentali dell'Unione europea

Art. 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.

Trattato sul funzionamento dell'Unione europea

Art. 16 (*ex* articolo 286 del TCE)

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.
Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea

Vanno inoltre citate le convenzioni specifiche in materia di trattamento automatizzato di dati a carattere personale, tra cui la c.d. Convenzione 108 del Consiglio d'Europa, emendata da un recente protocollo aggiuntivo.

Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale

STE n. 108 (Strasburgo, 28 gennaio 1981).

Protocollo di emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale

STCE n. 223 (Strasburgo, 10 ottobre 2018).

In un'ottica più specifica vanno infine ricordate alcune convenzioni internazionali dedicate al tema della tutela dei minori, contenenti disposizioni in materia di tutela della vita privata e della riservatezza dei minori stessi. Vengono in rilievo in tal senso l'art. 16 della Convenzione ONU sui diritti dell'infanzia e dell'adolescenza siglata a New York il 20 novembre 1989 e l'art. 8 della Convenzione ONU recante regole minime per l'amministrazione della giustizia minorile (c.d. Regole di pechino) del 29 novembre 1985.

Convenzione ONU sui diritti dell'infanzia e dell'adolescenza (New York, 20 novembre 1989)

Art. 16

Nessun fanciullo sarà oggetto di interferenze arbitrarie o illegali nella sua vita privata, nella sua famiglia, nel suo domicilio o nella sua corrispondenza, e neppure di affronti illegali al suo onore e alla sua reputazione. Il fanciullo ha diritto alla protezione della legge contro tali interferenze o tali affronti.

Convenzione ONU c.d. Regole di Pechino (New York, 29 novembre 1985) Regole minime per l'amministrazione della giustizia minorile

Art. 8 (Tutela della vita privata)

Il diritto del giovane alla vita privata deve essere rispettato a tutti i livelli per evitare che inutili danni gli siano causati da una pubblicità inutile e denigratoria. Di regola non dovrà essere pubblicata alcuna informazione che possa contribuire ad identificare un giovane autore di un reato.

2.2. Prospettiva di diritto interno

Per quanto concerne la prospettiva di diritto interno, il percorso che dalla direttiva 95/46/CE aveva condotto al Codice in materia di protezione dei dati personali adottato con d.lgs. 30 giugno 2003, n. 196 è stato contrassegnato da pochi riferimenti ai minori, relativi ad ipotesi specifiche, quali, ad esempio, la tutela della riservatezza con riferimento alle immagini e alle notizie relative ai minori in ambito processuale (art. 50 Codice Privacy) e il divieto di diffusione dei dati giudiziari dei minori (art. 52 Codice Privacy).

Con riferimento alla prospettiva interna si può, in linea generale, accennare ad alcune questioni che si possono definire "tradizionali" nell'ambito delle quali è stata fatta applicazione dei principi relativi alla tutela dei dati personali dei minori, anche sulla base delle convenzioni e della normativa internazionale in precedenza citate.

Una questione "classica" è rappresentata dalla pubblicazione di immagini e notizie relative ai minori, risolta sulla base dell'applicazione delle disposizioni di cui

- all'art. 10 Codice Civile (divieto di abuso dell'immagine altrui) che consente all'autorità giudiziaria di disporre la cessazione dell'abuso salvo il diritto al risarcimento del danno;
- all'art. 96 l. n. 633 del 1941 sulla protezione del diritto d'autore che vieta l'esposizione, la riproduzione, la messa in commercio del ritratto di una persona senza il consenso di questa salva la ricorrenza delle condizioni specifiche di cui al seguente art. 97;

– all'art. 4 del Codice in materia di protezione dei dati personali che consente l'identificazione dell'immagine del minore quale dato personale;
– all'art. 8 della Convenzione europea sulla salvaguardia dei diritti dell'uomo e delle libertà fondamentali e all'art. 7 della Carta dei diritti fondamentali dell'Unione europea sul rispetto alla vita privata e familiare;
– all'art. 16 della Convenzione di New York sui diritti dell'infanzia e dell'adolescenza sul diritto alla tutela della vita privata del minore.

Si riportano alcuni esempi di sentenze e provvedimenti nell'ambito dei quali si è fatta applicazione dei principi richiamati, in uno con il fondamentale principio guida costituito dalla tutela dell'interesse superiore del minore, per la risoluzione di controversie concernenti la pubblicazione di immagini e notizie di minori sui *social networks*.

• *Tribunale di Mantova 19 settembre 2017* (pubblicazione foto di figli minori su social network – ricorso *ex* art. 337 *quinquies*)

Tribunale di Roma, Sez. I civ., 23 dicembre 2017 (diffusione di immagini e notizie sulla vicenda giudiziaria relativa a minore su *social network* – ricorso *ex* art. 709 *ter* cpc – applicazione *astreinte ex* art. 614-*bis* cpc d'ufficio)

• *Tribunale Bari 7 novembre 2019* (pubblicazione immagini di adulto e figlio minore da parte ex compagna – cessazione condotta abusiva *ex* art. 10 cc. e *astreinte ex* art. 614-*bis* cpc)

È interessante notare come, in alcuni casi, ai fini dell'inibizione del comportamento lesivo, si sia fatta applicazione anche dell'*astreinte* o pena pecuniaria di cui all'art. 614-*bis* Codice Procedura Civile per ogni violazione o inadempimento successivo.

Vanno poi citate le questioni particolari rispetto alle quali sono state adottate specifiche disposizioni del Codice in materia di protezione dei dati personali concernenti i minori.

Viene in rilievo innanzitutto l'art. 50 sul divieto di pubblicazione di immagini o notizie di minori coinvolti in un procedimento giudiziario. Tale norma ha esteso il divieto già esistente in relazione al procedimento minorile, prevedendo il *divieto di pubblicazione e divulgazione con qualsiasi mezzo di notizie o immagini idonee a consentire l'identificazione di un minore* con riferimento *al coinvolgimento a qualunque titolo del minore in procedimenti giudiziari* anche *in materie diverse da quella penale,* e prevedendo che *la violazione del divieto di cui al presente articolo è punita ai sensi dell'articolo 684 del codice penale.*

Si riporta l'esempio di una decisione dell'Autorità Garante che ha fatto applicazione del divieto ai fini della soluzione di un reclamo concernente la pubblicazione da parte di un genitore sul proprio profilo *facebook* della propria sentenza di cessazione degli effetti civili del matrimonio, contenente dati personali di una minorenne:

• *Autorità garante della privacy, 23 febbraio 2017*

Ancora, deve farsi riferimento alla disposizione dell'art. 52 comma 5 sul divieto di diffusione dei dati giudiziari dei minori. Giova ricordare che l'art. 52, in materia di dati identificativi degli interessati, prevede in linea generale che l'interessato possa chiedere, prima della definizione del procedimento che lo riguarda, che, sulla sentenza o sul provvedimento sia apposta una annotazione volta a precludere, in caso di riproduzione del provvedimento, l'indicazione delle sue generalità e degli altri dati identificativi. La disposizione del comma 5 stabilisce che, anche in mancanza di tale annotazione, chiunque diffonda sentenze o provvedimenti dell'autorità giudiziaria sia tenuto ad omettere in ogni caso le generalità, altri dati identificativi, e altri dati anche relativi a terzi da cui possa desumersi anche indirettamente l'identità di minori o delle parti di procedimenti in materia di stato di famiglia e delle persone.

Eventuali eccezioni dovranno fondarsi su di una base giuridica specifica: può essere interessante a questo riguardo il riferimento all'art. 1 comma 334 della legge n. 160 del 2019 (legge di bilancio 2020 e bilancio di previsione 2020-2022) che ha stabilito l'esenzione dalle spese sanitarie per i minori privi di sostegno familiare, prevedendo a tal fine la trasmissione da parte del Ministero della Giustizia all'anagrafe degli assistiti del sistema tessera sanitaria dei dati giudiziari relativi ai minori privi di sostegno familiare (per i quali l'autorità giudiziaria abbia pronunciato un provvedimento *ex* art. 343 c.c. o 403 c.c. o *ex* art. 4 l. n. 184 del 1983).

3. Il GDPR: la tutela dell'azione dei minori nel mondo digitale

La novità del Regolamento generale sulla protezione dei dati personali è rappresentata dal fatto di aver disciplinato, per la prima volta, l'azione diretta dei minori nel mondo digitale, o, per rimanere al lessico del regolamento, con riferimento ai Servizi forniti dalle Società dell'informazione di cui all'art. 4. Tale disposizione richiama a sua volta la definizione di cui all'art. 1 par. 1 della Direttiva UE 2015/1535, ossia "*qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi*". Per quanto concerne l'ambito di applicazione, va rammentato che si tratta di una limitazione ulteriore rispetto a quella generale di cui all'art. 2 del Regolamento, concernente il trattamento interamente o parzialmente automatizzato di dati personali e il trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Alla base delle nuove disposizioni vi è una duplice consapevolezza, inerente, da un lato, allo sviluppo tecnologico di cui i nativi digitali sono grandi fruitori e nell'ambito del quale i dati personali costituiscono un bene economico primario e, dall'altro lato, alla evoluzione normativa e giurisprudenziale sul potere auto-deter-

minativo dei minori (alla base, ad esempio, del riconoscimento del diritto del minore ad essere sentito in ogni procedimento che lo riguardi e di determinati ambiti di autonomia del minore). Tale duplice consapevolezza si aggiunge alla funzione sociale del diritto alla protezione dei dati, espressa dal Considerando 4 del Regolamento, in base al quale il diritto alla protezione dei dati non è assoluto ma viene in rilievo nel bilanciamento con altri diritti ed interessi fondamentali, quali l'informazione, la sicurezza, etc. A fondamento delle nuove disposizioni vanno richiamati altresì gli sviluppi raggiunti oltreoceano, negli Stati Uniti, in cui ad oggi risultano localizzate le sedi principali delle più diffuse piattaforme on line, che hanno condotto, ancora nel 1998 all'emanazione del *Children's Online Privacy Protection Act* (c.d. COPPA) che aveva fissato in 13 anni l'età minima per il minore per prestare il consenso rispetto all'utilizzazione di dati per la fruizione di servizi.

I principi posti alla base delle nuove nuove disposizioni del GDPR in materia di minori sono espressi nei Considerando di seguito richiamati:

- C. 38: necessità di specifica protezione dei minori, in quanto meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia, nonché dei loro diritti in relazione al trattamento.
  Tale specifica protezione dovrebbe riguarda in particolare le seguenti attività: marketing / creazione di profili di personalità o di utente /raccolta dati personali all'atto dell'utilizzo di servizi forniti direttamente a un minore.
- C. 38: per usufruire di servizi di prevenzione o di consulenza destinati a minori non è necessario il consenso del titolare della responsabilità genitoriale.
- C. 58: principio della trasparenza e della necessità di un linguaggio semplice e chiaro che un minore possa capire facilmente.
- C. 65: diritto di ottenere la rettifica dei dati personali – «diritto all'oblio» – diritto alla cancellazione dei dati. Da assicurare in particolare se l'interessato ha prestato il proprio consenso quando era minore (indipendentemente dal fatto che non lo sia più nel momento in cui esercita il diritto alla cancellazione).
- C. 71: la «profilazione», ossia quel particolare tipo di trattamento automatizzato di dati personali che valuta aspetti personali al fine di effettuare analisi o previsioni (concernenti ad esempio il rendimento professionale, la situazione economica, la salute, le preferenze commerciali, gli spostamenti), non dovrebbe riguardare i minori.

Tali principi, fatta eccezione per quello sulla profilazione espresso nel C. 71, sono stati tradotti nelle seguenti specifiche disposizioni del GDPR:

- ART. 8

  Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione

(C38) (Art. 6, par. 1, lett. a) (Art. 4)
Riferimenti ai considerando e ad altre disposizioni del GDPR:

1. *Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.*
   Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.
2. *Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.*
3. *Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.*

• Art. 12 par. 1

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato
(C58)

1. *Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.*

• Art. 17 par. 1 lett. f)

Diritto alla cancellazione («diritto all'oblio»)
(C65) (Art. 8)

1. *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, se sussiste uno dei motivi seguenti:*
   a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
   b) l'interessato revoca il consenso su cui si basa il trattamento conforme-

mente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

3.1. Art. 8 GDPR: il consenso del minore in relazione ai servizi forniti dalle società dell'informazione.

L'art. 8 GDPR disciplina per la prima volta nel contesto europeo le condizioni applicabili al consenso dei minori in relazione ai servizi forniti dalle società dell'informazione (ossia, secondo la definizione data dall'art. 1 par. 1 della Direttiva UE 2015/1535, con riferimento a qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi).

Al paragrafo 1 la norma stabilisce innanzitutto l'età necessaria per esprimere il consenso prevedendo la liceità del trattamento se l'interessato ha compiuto i 16 anni (al di sotto, affinchè il trattamento sia lecito, il consenso deve essere espresso o autorizzato da chi esercita la responsabilità genitoriale). Il medesimo paragrafo prevede la possibilità di deroga da parte degli Stati membri, che possono fissare un'età diversa, purché non inferiore a 13 anni. La conseguenza dell'applicazione della possibilità di deroga è stata una mancanza di armonizzazione tra le discipline dei diversi Stati membri, che prevedono età differenziate per esprimere il consenso.

In Italia la deroga è stata esercitata all'art. 2 *quinquies* del Codice Privacy come modificato con d.lgs. n. 101 del 2018, fissando in 14 anni l'età necessaria per esprimere il consenso.

Le disposizioni del GDPR, se da un lato consentono un'azione diretta del minore, dall'altro prevedono una serie di salvaguardie:

- Art. 8 par. 1 La liceità del trattamento è riferita alla sola ipotesi di cui all'art. 6 par. 1 lett. a) ossia alla sola ipotesi di trattamento basato sul consenso dell'interessato;
- Art. 8 par. 2 È prevista una procedimentalizzazione più incisiva: "*il titolare del trattamento si adopera in ogni modo ragionevole per verificare che il*

consenso sia autorizzato o prestato dal titolare della responsabilità genitoriale in considerazione delle tecnologie disponibili"
È un obbligo che dovrebbe incidere sull'adozione delle garanzie di sicurezza di cui all'art. 32 GDPR e sulla Valutazione d'impatto (DPIA) di cui all'art. 35 GDPR;

- Art. 12 GDPR: Principio di trasparenza delle informazioni, le quali, in particolare laddove siano destinate a minori, devono essere espresse in un linguaggio semplice e chiaro, che l'interessato possa capire facilmente.

Il paragrafo 3 dell'art. 8 disciplina poi i contratti stipulati da un minore, stabilendo che *"il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto ad un minore"* e dunque le norme generali in materia di capacità d'agire (art. 2 Codice Civile).

Ci si chiede innanzitutto se non vi sia una contraddizione, nel senso che lo stesso contratto relativo all'utilizzazione dei dati personali necessari per usufruire del servizio rischierebbe di essere invalido. Si tratta di un tema su cui la dottrina si è interrogata e rispetto al quale allo stato non risultano pronunce; accedendo ad una interpretazione teleologicamente orientata, comunque, la norma dovrebbe essere intesa nel senso di fare riferimento a contratti diversi ed ulteriori, ad esempio relativi all'acquisto di beni o di altri servizi.

L'applicazione delle norme nazionali sulla validità, la formazione o l'efficacia di un contratto rispetto ad un minore comporta poi la possibilità di annullamento del contratto stipulato dall'incapace di agire. A questo riguardo dovrà comunque tenersi presente la possibilità di invocare la disposizione di cui all'art. 1426 Codice Civile, secondo cui il contratto non è annullabile se il minore ha con raggiri occultato la sua minore età; ancora, si dovrà considerare la possibile configurabilità di una responsabilità genitoriale da omesso controllo. Si può pensare alle ipotesi della utilizzazione da parte del minore della carta di credito intestata ai genitori o alla mancata attivazione da parte dei genitori di dispositivi di *parental control*.

3.2. Art. 17 GDPR: diritto all'oblio ed alla cancellazione dei dati personali dei minori.

Il principio di cui al Considerando 65 – secondo cui il diritto all'oblio ed alla cancellazione dei dati "*è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet*" – ha trovato attuazione all'art. 17 del Regolamento.

Il paragrafo 1 dell'articolo in esame prevede che *"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*", se sussiste uno dei motivi enucleati nelle varie lettere indicate. La lettera f) fa in particolare riferimento all'ipotesi in cui "*i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo".*

Il fatto che il consenso sia stato prestato quando l'interessato era un minore costituisce quindi una ragione specifica di esercizio del diritto alla cancellazione dei dati, che va ad aggiungersi alle ulteriori ipotesi previste dal par. 1 (ad esempio il fatto che i dati non siano più necessari per le finalità per cui sono stati raccolti, la revoca del consenso, l'opposizione al trattamento, l'illiceità del trattamento, etc.), e nella ricorrenza della quale la richiesta deve essere accolta indipendente dalla sussistenza delle altre condizioni, compresa la liceità del trattamento.

Applicando il principio enucleato al C. 65, il diritto deve poter essere esercitato anche quando l'interessato non sia più un minore ed anche qualora il consenso sia stato espresso dagli esercenti la responsabilità genitoriale

4. Limiti della disciplina del GDPR a tutela dei minori e spunti conclusivi

Il Regolamento generale sulla protezione dei dati personali, pur avendo sicuramente introdotto delle disposizioni innovative in tema di tutela dei dati personali dei minori, presenta anche importanti delle lacune, da più parti segnalate.

Si può considerare ad esempio la previsione di cui all'art. 9 del Regolamento in tema di trattamento di categorie particolari di dati personali, costituiti dai dati "*che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".* Secondo quanto stabilito dalla norma citata il trattamento di tali dati è vietato, salvo ricorrano particolari eccezioni, quali ad esempio il consenso esplicito dell'interessato (lett. a) o il fatto che i dati siano stati resi manifestamente pubblici dall'interessato (lett. e), come in caso di pubblicazione nei *social networks*. Le voci critiche ritengono che sarebbe stata quantomeno opportuna una previsione specifica in tema di dati particolari dei minori.

Si è già ricordato, poi, come il principio espresso al Considerando 71 in tema di attività di profilazione, "*che non dovrebbe riguardare un minore*", non sia stato tradotto in un divieto espresso. Possono al riguardo supplire i Codici di condotta approvati dalle associazioni e dagli organismi di categoria ai sensi dell'art. 40 GDPR, ma è evidente la lacuna del GDPR.

Soprattutto va ricordato che il GDPR disciplina, con specifico riferimento ai minori, i soli servizi offerti dalle società dell'informazione, pur essendo i minori ampi fruitori del mondo digitale ampiamente inteso. Trattasi in realtà di un limite ricorrente rispetto ad ogni ipotesi di normativa diretta a disciplinare un settore influenzato dall'innovazione tecnologica, essendo esposta al rischio di risultare anacronistica rispetto all'evoluzione della tecnica e delle sue applicazioni pratiche.

Si pongono ad esempio questioni aperte di tutela in relazione alle nuove frontiere dell'intelligenza artificiale, dell'*Internet of Things,* dei dispositivi domotici, degli *smart toys* (mondi in cui gli oggetti cessano di essere "inanimati", venendo dotati di intelligenza artificiale e connessi alla rete), della *block-chain* e degli *smart contracts*.

In chiusura si possono quindi indicare alcuni spunti ulteriori di regolamentazione in ambito internazionale e rispetto a recenti proposte legislative europee.

Nell'ambito del Consiglio d'Europa vengono in rilievo le Linee guida, adottate con Raccomandazione del Comitato dei Ministri n. 7 del 4 luglio 2018, per rispettare, proteggere e realizzare i diritti del bambino nell'ambiente digitale[4]. La Raccomandazione, di cui esiste anche una versione a misura di bambino, contiene una parte specifica relativa a *privacy* e protezione dati. Per supportare l'applicazione della Raccomandazione, il 10 dicembre 2020 è stato poi pubblicato il Manuale per i decisori politici sui diritti del bambino nell'ambiente digitale[5]. Come noto, le raccomandazioni costituiscono strumenti di *soft-law,* non vincolanti, ma possono comunque venire in considerazione in chiave interpretativa.

Per quanto riguarda infine le prospettive future in ambito unionale, andranno in particolar modo monitorate:

– la Proposta di Regolamento sulla Governance dei dati (*Data Governance Act*) presentata dalla Commissione Europea presentato il 25 novembre 2020 nell'ambito della Strategia europea dei dati;
– la Proposta di Regolamento sui Servizi Digitali (*Digital Services Act*) e la Proposta di Regolamento sui Mercati Digitali (*Digital Markets Act*) entrambe presentate dalla Commissione Europea il 15 dicembre 2020 nell'ambito della Strategia digitale europea.

[4] CM/Rec(2018)7 Linee guida per rispettare, proteggere e realizzare i diritti del bambino nell'ambiente digitale (adottata il 4 luglio 2018).
https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

[5] Manuale per i decisori politici sui diritti del bambino nell'ambiente digitale (presentato il 10 dicembre 2020) https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8

Armando Spataro

Il dovere di riservatezza nell'attività giudiziaria

Presentazione

Le modalità di pubblica comunicazione dei magistrati hanno dato luogo a frequenti critiche secondo cui essi parlerebbero per rafforzare il peso dell'accusa o la propria immagine, nonostante il dovere di riservatezza cui sono tenuti. Si tratta di accuse quasi sempre infondate, ma che traggono spunto da innegabili criticità: basti pensare alla prassi delle conferenze stampa teatrali e dei comunicati stampa per proclami, o all'autocelebrazione delle proprie inchieste con connesse accuse a chi si permette di esprime dubbi e critiche. Bisogna spiegare ai magistrati "come non si comunica", convincendoli ad evitare i tentativi di "espansione" a mezzo stampa del proprio ruolo fino ad includervi quelli degli storici e dei moralizzatori della società. Il dovere di informare è naturalmente irrinunciabile, purchè esercitato nei limiti della legge, del rispetto della privacy e delle regole deontologiche, ma è anche necessario che i magistrati si guardino bene dal contribuire a rafforzare un'ormai evidente degenerazione informativa, che spesso determina febbre "giustizialista", alimentata da mostruosi "talk-shaw" ed attacchi alla politica ingiustificatamente generalizzati. I magistrati non sono ovviamente gli unici responsabili di questa pericolosa deriva cui contribuiscono anche strumentalizzazioni ad opera di appartenenti alle categorie degli avvocati, dei politici e degli stessi giornalisti che spesso producono informazioni sulla giustizia prive di approfondimento e di verifiche, e che sono caratterizzate dalla ricerca di titoli e di forzature delle notizie al solo scopo di impressionare il lettore. È necessaria, dunque, per venir fuori da questo preoccupante labirinto, una riflessione comune su informazione e giustizia tra magistrati, avvocati e giornalisti.

Allegato: Le direttive del Proc. della Repubbl. di Torino sui rapporti con gli organi di informazione

Premessa

Va subito precisato che questo intervento, fondato sull'esperienza professionale e personale dell'autore, riguarda problematiche di rilevanza pratica per giudici, pubblici ministeri ed avvocati che si occupano della materia penale. Non

contiene, pertanto, approfondimenti giuridici in tema di segreto investigativo (assoluto o parziale) e di punibilità per le relative violazioni.

Il corretto rapporto tra giustizia ed informazione-comunicazione è oggi uno dei pilastri su cui si fonda la credibilità dell'amministrare giustizia. All'opposto, la comunicazione scorretta ed impropria genera tra i cittadini errate aspettative e distorte visioni della giustizia, in sostanza disinformazione, così determinando ragioni di sfiducia nei confronti della magistratura e conseguente perdita della sua credibilità.

Non a caso il Consiglio Superiore della Magistratura, pur nell'ambito di un interventismo talvolta eccessivo, ha emanato nella seduta dell'11 luglio 2018 le Linee Guida per l'organizzazione degli Uffici Giudiziari "ai fini di una corretta comunicazione istituzionale", quale espressione della necessità di trasparenza, controllo sociale e comprensione – da parte dei cittadini – della giustizia intesa come servizio, come funzione, come istituzione.

Del resto, come è stato osservato[1], il magistrato non è più, in sé, simbolo di prestigio sociale e, tanto meno, di autorevolezza, fiducia, credibilità. La percezione sociale del magistrato e della giustizia – e dunque la maggiore o minore fiducia, il maggiore o minore rispetto, la maggiore o minore credibilità – si nutre sempre di più anche del "costume giudiziario", ovvero di come i magistrati si pongono, parlano, scrivono, si comportano, e si relazionano con le parti del processo e con il pubblico.

Peraltro, si tratta di condotte che all'evidenza devono sempre rispettare la *privacy* delle parti a vario titolo coinvolte nei processi penali, la cui tutela è ormai oggetto di ripetuti interventi legislativi, anche a livello sovranazionale.

La giustizia viene comunicata quotidianamente all'esterno con vari strumenti, inclusi avvisi di garanzia, provvedimenti cautelari, sentenze, ma oggetto di questo intervento non sono le tecniche di redazione dei provvedimenti giudiziari, quanto le modalità di comunicazione esterna attraverso interviste, conferenze, comunicati-stampa che spesso appaiono la spia di diffuse propensioni dei magistrati ad accrescere, per quelle vie, la popolarità della propria immagine, anche a costo di non rispettare il dovere di riservatezza proprio dell'attività giudiziaria.

Le conseguenze di tali modalità di comunicazione fanno sì che i principi su cui la corretta informazione si fonda non possono essere appannaggio soltanto di pochi – capi degli uffici e loro delegati – ma dev'essere una consapevolezza (e una competenza) "diffusa" ad ogni livello, pur se, anche in ragione dell'esperien-

[1] Documento di presentazione di un Corso di studi tenutosi nel giugno 2017 presso la Scuola Superiore della Magistratura di Scandicci.

za professionale di chi scrive, appresso si parlerà soprattutto dei doveri e degli errori dei P.M., i magistrati più esposti a critiche per le modalità comunicative di cui sono spesso protagonisti.

Sarà utile, dunque, passare in rassegna le più diffuse criticità del modo di comunicare di molti magistrati e le accuse che conseguentemente piovono addosso all'ordine giudiziario[2]. Bisogna precisare, però, che non è accettabile alcuna generalizzazione di vizi e di certe pessime abitudini di alcuni magistrati, anche perché essi non sono certo gli unici protagonisti di una deriva insopportabile che ormai si manifesta sul terreno dei rapporti tra giustizia ed informazione: intendo riferirmi, anche in questo caso evitando rischi di ingiuste generalizzazioni, a certi atteggiamenti che sono propri di forze di polizia giudiziaria, di avvocati, politici e perfino, se non soprattutto, di giornalisti.

Il tema in questione va comunque esaminato con freddezza e ragione partendo da un'affermazione netta ed inequivoca: l'informazione sulla giustizia è certamente necessaria, rivestendo anzi la dimensione di un dovere da parte di chi deve diffonderla e di un diritto da parte di chi ne è destinatario, ma dell'uno e dell'altro occorre precisare contenuti e confini, anche nel rispetto dei principi che disciplinano la tutela della *privacy*.

1. Si parla per rafforzare il peso dell'accusa?

Una delle accuse, spesso strumentali, rivolte ai magistrati è quella secondo cui – specialmente se pubblici ministeri – essi si servirebbero dei media per rafforzare il peso dell'accusa in vista del processo.

---

[2] Come si vedrà si tratta di condotte che potrebbero anche integrare estremi di responsabilità disciplinare, ove si tenga che presente che l'art. 2 del d.lgs. 23 febbraio 2006 n. 109 e successive modifiche, prevede tra l'altro che costituiscono illeciti disciplinari nell'esercizio delle funzioni:
…omissis…
u) la divulgazione, anche dipendente da negligenza, di atti del procedimento coperti dal segreto o di cui sia previsto il divieto di pubblicazione, nonché la violazione del dovere di riservatezza sugli affari in corso di trattazione, o sugli affari definiti, quando è idonea a ledere indebitamente diritti altrui;
v) pubbliche dichiarazioni o interviste che riguardino i soggetti coinvolti negli affari in corso di trattazione, ovvero trattati e non definiti con provvedimento non soggetto a impugnazione ordinaria, quando sono dirette a ledere indebitamente diritti altrui nonché la violazione del divieto di cui all'articolo 5, comma 2, del decreto legislativo 20 febbraio 2006, n. 106 (2);
aa) il sollecitare la pubblicità di notizie attinenti alla propria attività di ufficio ovvero il costituire e l'utilizzare canali informativi personali riservati o privilegiati.

Personalmente, pur dando per scontati vizi e pessime abitudini di cui si parlerà, non credo affatto che sia diffusa tra i pm la convinzione che, incrementando il rilievo mediatico delle proprie inchieste, sia possibile far crescere le probabilità di ottenere la condanna degli imputati, specie in processi difficili.

Se qualche pubblico ministero la pensasse in questo modo, il che non può essere in assoluto escluso, egli non meriterebbe stima e fiducia, ma solo di essere additato come l'opposto del modello di Pubblico Ministero che il nostro sistema prevede. Sempre che non violi norme disciplinari (si rinvia sul punto alla nota n. 2 in pagina precedente) o penali: in tal caso meriterebbe anche severe condanne.

Comunque, non credo affatto che il possibile protagonismo di certi pubblici ministeri possa produrre conseguenze sulle decisioni dei Tribunali, pur se non possono non essere stigmatizzate anche le dichiarazioni di alcuni giudici che, dopo la lettura del dispositivo, hanno sia pur sommariamente anticipato la motivazione di una sentenza. In generale, va detto che i giudici sono piuttosto le vittime potenziali del clamore mediatico. Basti pensare al caso di un'assoluzione che faccia seguito ad una ormai diffusa convinzione di colpevolezza degli imputati: il giudice diventa facilmente bersaglio di dure accuse, tra cui quella di non avere voluto affermare la verità a causa di condizionamenti o di mancanza di coraggio o per timore di ripercussioni sulla propria carriera.

Ecco perché credo che il "giusto processo", specie in casi eclatanti, sarebbe tale anche grazie a notizie giuste e vere, conoscibili entro i limiti previsti per le varie fasi processuali e contenenti esclusivamente riferimenti ai fatti che sono oggetto del processo.

2. I magistrati parlano per rafforzare la propria immagine?

La tendenza al protagonismo individuale è, in effetti, un problema reale connesso alla convinzione di alcuni Pm di potersi proporre al Paese, attraverso la diffusione mediatica di notizie sulle proprie indagini, spesso enfatizzate, come eroi solitari, unici interessati alle verità che i poteri forti intendono occultare.

Sono preferibili, invece, quei magistrati che non cercano consenso (specie nelle piazze gremite) e che lavorano con riservatezza e determinazione: il modello ideale è stato, e rimane, Francesco Saverio Borrelli il quale ripeteva che la solitudine è lo stato ordinario del nostro lavoro. Il nostro dovere è quello di indagare con determinazione, senza fermarci dinanzi ad ostacoli di qualsiasi natura, al solo fine di provare la verità dei fatti e la responsabilità di chi ne è autore.

3. L'informazione necessaria non è quella delle conferenze stampa teatrali e dei comunicati stampa per proclami

Tuttavia l'informazione serve ai cittadini, ma va data con misura e quando lo sviluppo delle indagini lo consente. Cerco di spiegarlo con esempi concreti.

Partiamo, intanto, dal dovere deontologico che esiste per tutti i magistrati di non parlare dei processi in corso e da quello dei dirigenti di assicurare una corretta informazione per fatti di pubblico rilievo rispettando i doveri di verità e sobrietà informativa, specie quando i fatti sono oggetto di indagine e non ancora di una sentenza, sia pure di primo grado. Per i dirigenti degli Uffici Giudiziari, in particolare per i Procuratori della Repubblica, esiste anche il dovere di intervenire per correggere le *fake news:* serve farlo con misura e precisione per evitarne l'enfatizzazione, così come per far fronte al rischio di "pregiudizio alle indagini, ai diritti delle persone coinvolte, all'immagine di imparzialità e correttezza del singolo magistrato, dell'ufficio giudiziario e, nei casi più gravi" della stessa funzione giudiziaria"[3].

Quanto alle conferenze stampa, mi permetto subito un riferimento personale: per il periodo in cui ho diretto la Procura della Repubblica di Torino, cioè dalla fine del mese di giugno del 2014 fino al dicembre del 2018, ne ho tenute solo tre: la prima per denunciare pubblicamente, insieme agli Avvocati, il grave deficit di personale amministrativo dell'Ufficio; la seconda per illustrare i risultati ostensibili delle indagini sui gravi fatti verificatisi in Torino, in Piazza San Carlo, il 3 giugno 2017 (che avevano scosso l'intera città) e l'ultima per presentare pubblicamente le direttive emesse il 9 luglio 2018 in tema di priorità da accordare alla trattazione dei reati connotati da odio razziale ed al fine di velocizzare le procedure relative ai ricorsi avverso il rigetto delle richieste di protezione internazionale (argomenti, cioè, che richiamavano attualità e diritti fondamentali delle persone).

Non è a mio avviso apprezzabile, invece, la pratica delle conferenze stampa che vedono appartenenti alle forze di polizia schierati in divisa al fianco dei magistrati o dietro di loro: l'ho fatto una sola volta in oltre 40 anni e me ne sono presto pentito. Preferisco comunicati stampa sobri ed essenziali che hanno il pregio di diffondere parole e notizie precise, senza possibilità di interpretazioni forzate. Come avviene a Torino[4], i Pubblici Ministeri, anche per dare ulteriore concretezza al principio della direzione della Polizia Giudiziaria che la Costituzione ed il

---

[3] Citata delibera del CSM dell'11 luglio 2028.

[4] Si rimanda sul punto a quanto si dirà più avanti in ordine ai Criteri di organizzazione della Procura della Repubblica di Torino, varati dallo scrivente l'8.10.2018, di cui viene qui allegata la parte concernente i rapporti con gli organi di informazione e le disposizioni in proposito vigenti per i componenti dell'Ufficio e la polizia giudiziaria.

Codice di rito loro attribuiscono, dovrebbero sempre ricevere preventivamente dai vertici locali dei presidi di polizia giudiziaria operanti nel circondario o, a seconda delle competenza, nel Distretto, i comunicati stampa che essi intendono diffondere in ordine a rilevanti indagini effettuate e, in caso di necessità, sottoporli alle valutazioni del Procuratore. Tale prassi è utile anche per pervenire a contenuti, modalità e tempi della diffusione delle notizie di interesse pubblico improntati anche al rispetto dei diritti e delle garanzie spettanti agli indagati per qualsiasi reato.

In sostanza, vanno evitati eccessi comunicativi della polizia giudiziaria (spesso dovuti al fine di acquisire titoli utili per la progressione in carriera, mediante visibilità e impatto mediatico delle proprie attività) o anticipate diffusioni di notizie – con o senza tweet – che possono determinare il rischio di pregiudicare il buon esito delle operazioni. Queste, infatti, non si esauriscono nel momento dell'arresto di un ricercato o dell'avvenuta effettuazione di controlli e perquisizioni: talvolta, ad es., l'arrestato può chiedere di essere interrogato ed occorre che il PM vi provveda subito se l'atto si presenta utile. Altre volte il materiale sequestrato può determinare ulteriori urgenti attività. E gli esempi potrebbero continuare. È importante, dunque, che PM, Polizia Giudiziaria e vertici delle strutture operanti condividano la cultura della informazione appropriata per contenuto e tempistica, che può persino essere frutto di oculata elaborazione di strategie investigative, quando, ad es., si diffonde *ad hoc* una specifica notizia perché ciò può determinare utili ed importanti sviluppi.

Il più efficace esempio di tale cultura è stato da me vissuto il 4 aprile 1981, data dell'arresto a Milano di Mario Moretti ed Enrico Fenzi, vertici delle B.R.. L'arresto era ovviamente clamoroso, anzi storico e, come sempre in questi casi, gli organi di polizia avevano il comprensibile desiderio di convocare conferenze stampa o diramare comunicati. D'altro canto, non potevo permetterlo finché non fossi stato certo che la divulgazione della notizia non avrebbe danneggiato possibili sviluppi investigativi. Ma arrivò la risolutiva telefonata del ministro dell'Interno Virginio Rognoni che mi chiamò personalmente: ero un giovane p.m. di trentadue anni e mi disse: «Lei sa quanto per noi sia importante l'arresto di Moretti e quanto lo sia darne la notizia. Però prima di ogni altra esigenza vengono quelle dell'autorità giudiziaria. Lei faccia tutto quello che ritiene necessario, però le rivolgo una preghiera: quando avrà finito, mi chiami personalmente per dirmi che posso dare la notizia alla stampa. Vorrei ricevere questo nulla osta direttamente dalla sua voce, non da altri». Lo ringraziai. Lavorammo intensamente per ore: interrogammo Moretti e Fenzi e studiammo poi le poche carte che avevano addosso, dopodiché telefonai a Rognoni. Il ministro mi ringraziò e diffuse la notizia. Questo era Virginio Rognoni, un ministro di esemplare correttezza e cultura, che non

avrebbe mai usato, in simili casi, cellulari, sms e tweet, neppure se fossero esistiti nel 1981.

Quanto ai comunicati ed alle conferenze stampa, è però inaccettabile la prassi di quei pubblici ministeri che, presentando pubblicamente le proprie indagini, usano lanciare veri e propri proclami del tipo "si tratta della più importante indagine antimafia del secolo" o "finalmente abbiamo scoperto la mafia al Nord", così proponendosi come icone – categoria purtroppo in espansione – per le piazze plaudenti. Addirittura, nel dicembre del 2019, un Procuratore Distrettuale della Repubblica ha lamentato il fatto che i quotidiani nazionali, salvo poche eccezioni, avrebbero dato poco risalto ad una certa indagine condotta dal suo ufficio da lui ritenuta di storico rilievo, arrivando in proposito ad affermare, in una intervista televisiva, che "*i giornali nazionali hanno boicottato la notizia*". Ed a fronte di alcune critiche mosse a tali modalità comunicative, è stato sostenuto che esse possono rivestire lo scopo nobile di sollecitare l'attenzione dei cittadini e la loro reazione contro la mafia. Affermazioni non condivisibili posto che una conferenza stampa o dichiarazioni su specifiche indagini non sono certo equiparabili ad un dibattito pubblico su mafia e legalità. Ed in ogni caso, qualsiasi tipo di enfasi comunicativa non è condivisibile, specie se proviene da magistrati!

Recentemente, sono stati anche diffusi comunicati in forma criticabile: troppo lunghi nel testo e perfino contenenti, da un lato, brani oggetto di conversazioni registrate durante le indagini preliminari, dall'altro spunti critici verso giudici o avvocati, oppure affermazioni apodittiche quasi che le tesi dei pm esposte nei comunicati rappresentino la verità inconfutabile, definitivamente accertata, insomma un anticipo di sentenza. Niente di più lontano, insomma, dal senso del limite e dall'etica del dubbio cui devono conformarsi le parole di un pubblico ministero prima della decisione del giudice.

I comunicati stampa, invece, oltre a dover essere ovviamente chiari, sintetici ed efficaci, non possono che riguardare informazioni di effettivo interesse pubblico e contenere brevi riferimenti alla natura dei reati per cui si procede, alla provvisorietà delle valutazioni del giudice (non del PM) sulle responsabilità delle persone sottoposte a misura cautelare, evitando citazione di nomi e diffusione di fotografie o comunicazione di dati sensibili almeno ove tali nomi ed immagini non siano noti per altri fatti oggettivi (ad es., arresti in flagranza o diffusione di notizie, come è avvenuto, da parte degli stessi indagati).

Particolare attenzione va ovviamente riservata alla necessità di evitare in qualsiasi modo che notizie segrete o comunque riservate possano essere anche indirettamente propagate o intuite: i danni alle indagini sono in questi casi evidenti e finiscono con il legittimare le accuse sistematicamente rivolte ai magistrati – in quanto detentori delle notizie – di determinarne le cd. "fughe".

4. No all'"espansione" a mezzo stampa del ruolo dei magistrati

Vanno anche criticate altre improponibili modalità di comunicazione attuate e perseguite da quanti, anche in un passato non troppo lontano che purtroppo non appare ancora abbandonato, hanno affermato, in una logica di autolegittimazione preventiva e di ricerca del consenso delle folle, che il proprio lavoro investigativo, pure in caso di eventuale insuccesso processuale, sarebbe comunque servito a ricostruire la storia del Paese o a moralizzarlo: con ciò dimenticando che l'oggetto dei processi penali non può mai essere una pura valutazione storica dell'epoca in cui i fatti si collocano o un mero giudizio etico, politico o di opportunità di certi comportamenti, mentre lo è solo l'accusa di avere violato specifiche norme penali.

Va cioè respinta l'immagine del magistrato unico (o quasi) depositario della morale collettiva. Il compito dei magistrati non è quello di formulare ipotesi affascinanti, ma di mettere a nudo la verità con prove inconfutabili. E questo comporta un limite: se quelle prove non si raggiungono, il magistrato, pur se convinto del fondamento della ipotesi accusatoria da cui si è mosso, ha esaurito il suo ruolo, deve considerare i limiti della giustizia umana e se è un pubblico ministero deve saper ragionare come un giudice e comunque rimettersi alla decisione finale dei Tribunali e delle Corti rispettandola fino in fondo. Altrimenti, finirà con il favorire proprio quei poteri criminali che si propone di contrastare: l'aspirante moralizzatore diventerà forse una icona per una parte del Paese ma certamente l'esercizio del potere giudiziario rischierà di apparire arbitrario, sganciato da regole certe, incomprensibile. Ed il pubblico ministero o il giudice, approdato ad un ruolo che non gli appartiene, finirà con il dare la sensazione di essere stato condizionato da quell'abbraccio della folla che ha cercato o non evitato e, involontariamente, finirà con il compromettere l'autorevolezza della giustizia.

Come invece ha scritto il grande giurista elvetico Dick Marty[5], bisogna essere (e dimostrare di essere) «prudenti nel giudicare e attenti nel non lasciarsi trascinare dal pensiero dominante, che tende a interpretare i fatti come un conflitto ineluttabile tra bene e male, tra buoni e cattivi».

Tocca allo storico o alla politica, invece, analizzare le sentenze e gli atti processuali e trarne conclusioni che riguardano le loro competenze ed il loro ruolo. E se da un'indagine o da un processo emergono comportamenti di indagati ed imputati eticamente o deontologicamente riprovevoli, toccherà ad altri valutarli, e se gli imputati sono politici o aspiranti tali, toccherà innanzitutto agli elettori, prima del voto, capirne e conoscerne la natura, poichè anche per i cittadini esiste

[5] "Una certa idea di giustizia" (Ed. Casagrande 2019).

il dovere della effettiva conoscenza di fatti e persone, specie se per queste ultime è chiamato ad esprimere il voto.

Non potrò dimenticare l'amico e collega fiorentino Gabriele Chelazzi che, dinanzi alla Commissione Parlamentare Antimafia nel 2002, espose la sua tesi secondo cui non si può chiedere al giudice di andare oltre una certa soglia, avendo egli l'obbligo di provare la responsabilità degli autori dei reati con riscontri oggettivi.

E – concludeva Chelazzi – le connessioni e le conseguenze sulla società di fatti di grave entità, come ad es. le stragi, non possono che essere accertate da una commissione parlamentare, competente per approfondimenti sotto altri profili.

5. L'esposizione mediatica, frutto della degenerazione informativa, può determinare febbre "giustizialista"?

Probabilmente i comportamenti sin qui descritti sono conseguenti alla progressiva degenerazione dei rapporti tra giustizia e informazione manifestatasi negli ultimi venticinque anni, soprattutto a seguito del rilievo che hanno assunto indagini e processi penali nella vita politica italiana.

Di qui il moltiplicarsi di non pochi casi di eccesso di protagonismo da parte di alcuni pubblici ministeri, sia pure, come si è detto, senza ricadute negative sulla serenità dei giudici.

Minoranze di colleghi, però, indipendentemente dalla loro anzianità, manifestano talvolta eccessiva attenzione al rilievo mediatico del proprio lavoro, il che è anche effetto di involuzioni e cambiamenti nel modo di fare giornalismo: la pubblicazione della notizia di una indagine sui giornali, specie se con modalità tali da captare l'attenzione del lettore, rischia in tal modo di diventare per molti più importante della futura sentenza, di cui qualche giudice – come prima si è detto – ha talvolta persino anticipato la motivazione.

Da tutto ciò deriva un'altra accusa che viene rivolta ai magistrati: l'enfasi con cui certe indagini vengono rappresentate dalla stampa rischia di favorire il diffondersi di una "febbre giustizialista" nell'opinione pubblica, anche al di là degli effetti reali sullo svolgimento dei processi.

Ad esempio, si assiste spesso a processi mediatici ed alla costruzione di verità alternative rispetto a quelle accertate o da accertare nei dibattimenti: in particolare, trovano ampio ed immediato spazio le "verità" che si fondano su misteri senza fini, nell'ambito dei quali tutto si lega: qualcuno ha recentemente affermato che CIA, KGB, Mossad, Servizi Segreti italiani, massoneria, Cosa Nostra, 'Ndrangheta e Camorra, settori deviati della polizia e dei carabinieri furono gli organizzatori del sequestro di Moro e della strage della sua scorta cui aveva materialmente

partecipato almeno un rappresentante di ciascuna di tali "entità". Questa tesi – che ha spopolato e passa ormai per verità finalmente accertata – è maturata nella Commissione Parlamentare Stragi e Terrorismo in cui operano, come "consulenti", alcuni magistrati. E cosa dire del nesso che qualcuno ha affermato esistere tra la caduta del muro di Berlino, lo stesso sequestro Moro e la strage di Falcone, Borsellino e delle loro scorte? E le teorie su Piazza Fontana e sull'11 settembre? E perché, secondo un noto magistrato esperto di mafia, Matteo Messina Denaro sarebbe ancora latitante? Perché – ha dichiarato nel 2019 il magistrato in una intervista televisiva – "conosce troppi segreti!", così lasciando credere che forze di polizia ed altre Istituzioni omettono dolosamente di arrestarlo per evitare che Messina Denaro riveli quei segreti, così cedendo ai suoi ricatti! Mi fermo qui. Ma tant'è: basta il titolo ad effetto per rendere credibili costruzioni alternative della verità e processi mediatici. Ed è grave, a mio avviso, che certe teorie trovino spazio anche in ambiti istituzionali: basti pensare anche a quelle prive di qualsiasi fondamento che l'Ordine dei Giornalisti di Milano ha messo in campo a proposito dell'omicidio Tobagi, con l'avallo di un magistrato intervenuto in occasione della loro pubblica presentazione, nonostante molte sentenze definitive le avessero già del tutto smentite.

Anche in relazione alla logica sottesa alla esaltazione di certi presunti misteri, in sostanza, è possibile individuare contributi non secondari di magistrati che spesso richiamano responsabilità di imprecisate entità esterne e dei soliti "poteri forti", senza nome e senza volto, così fungendo da interlocutori del peggiore giornalismo, quello lontano anni luce dal vero giornalismo d'inchiesta di cui ovunque vi è bisogno.

Vale anche per i magistrati, dunque, il motto che i giornalisti inglesi usano per stigmatizzare quei loro colleghi che rifiutano di accertare/accettare il reale andamento dei fatti pur di non indebolire le loro fantasiose ipotesi: «Non permettere ai fatti di rovinare una bella storia!».

6. Magistrati, tra i "nuovi mostri dei talk-shaw"[6]. Le interviste-spettacolo

La presenza eccessiva di alcuni magistrati o ex magistrati nei talk show televisivi, che ormai ammorbano le serate degli italiani, costituisce un' ulteriore ragione di perdita di credibilità dell'ordine giudiziario: sembra impossibile che tanti colleghi non si rendano conto del fatto che l'inflazione di interviste e di-

[6] Si tratta di espressione che costituisce il titolo di un articolo, per altro non certo riferibile solo a magistrati, a firma di Andrea Miniz, pubblicato su Il Foglio dell'1.12.2018.

chiarazioni, specie se riferibili ad inchieste in corso, costituisce un fattore delegittimante della nostra funzione, così come quelle che anche su altri temi – dalle riforme della giustizia alle seriali accuse di clientelismo rivolte alle componenti dell'A.N.M. – vengono interrotte solo dagli applausi "ordinati" a comando negli studi televisivi.

Si pensi alle numerose interviste di pubblici ministeri che hanno criticato la riforma delle intercettazioni telefoniche trascurando almeno due decenni di dibattito attorno alla condivisa necessità di evitare la indebita diffusione di conversazioni non pertinenti alle indagini. Affermazioni immotivate come quella secondo cui, a seguito della riforma Orlando, sarebbe la polizia giudiziaria a decidere cosa rendere noto e cosa segretare, oltre a dimostrare una non corretta visione del ruolo di direzione della polizia giudiziaria che Costituzione e Codice di rito affidano al PM[7], sono servite a far riemergere la diffusa convinzione secondo cui i giornali hanno diritto a pubblicare subito tutto ciò che viene registrato e che ritengano rilevante, come se le intercettazioni delle comunicazioni fossero a ciò finalizzate, anziché alla ricerca delle prove per i reati per cui si procede.

Si sono anche visti magistrati sottoposti a protezione per i rischi connessi alla loro attività professionale rilasciare interviste in uno spazio aperto, circondati dai poliziotti di scorta che guardavano in alto, verso i muri del vicino Palazzo di giustizia, evidentemente alla ricerca di cecchini. Possiamo permetterci rappresentazioni simil-teatrali quando parliamo ai cittadini di temi delicati e importanti? E se rischi esistono, non è meglio rilasciare interviste nel proprio ufficio anziché all'aperto, mentre si è circondati dagli uomini di scorta?

Connesso al tema delle interviste-spettacolo è quello della costruzione e del mantenimento di canali informativi privilegiati tra magistrati ed esponenti del mondo dell'informazione, che – come ammonisce il CSM – producono discriminazione tra giornalisti e testate. Ricordo quando, da Procuratore Aggiunto a Milano, ebbi a ricevere nel mio ufficio un giovane giornalista che, presentandosi come nuovo addetto della sua importante testata alle cronache giudiziarie milanesi, mi rassicurò sul fatto che avrebbe mantenuto segreta la fonte di ogni notizia riservata che gli avrei passato. Mentre lo sbattevo fuori dall'ufficio, pensai che qualcuno doveva avergli detto che così si fa con i magistrati e che i magistrati lo accettano e magari lo gradiscono. E non è difficile ipotizzare che, purtroppo, ciò possa effettivamente avvenire fino a determinare l' "abbandono" di uno dei più importanti obiettivi che le corrette modalità di comunicazione impongono, cioè

[7] Solo un P.M. non del tutto capace di dirigere la polizia giudiziaria, infatti, può lasciarsi da questa dettare o imporre (anche fraudolentemente) le scelte di pubblicazione ed utilizzo delle conversazioni intercettate.

quello della massima spersonalizzazione delle notizie: ciò significa, ad es., che si può ben dare informazione – nei limiti sin qui precisati – circa un'indagine di pubblico interesse, ma questa deve essere attribuita all'Ufficio e non al singolo pubblico ministero che l'ha condotta.

7. Gli attacchi alla politica ingiustificatamente generalizzati

In un suo famoso pezzo dell'88, *Political world,* il premio Nobel Bob Dylan sostiene – in sintesi – che la politica vuole la sconfitta degli altri e l'impunità per sé. Non la penso affatto così e mi spiace dissentire, sia pure per una sola volta, dalla mia stella polare, il menestrello di Duluth. Battute a parte, dissento anche dai tanti colleghi che la pensano allo stesso modo e che lo ripetono in ogni tipo di pubblica esternazione. Io penso che la politica meriti rispetto e costituisca un'alta funzione, sia pur carica di criticità e (come anche la magistratura) frequentemente "praticata" da persone che non meritano la fiducia degli elettori.

Dunque, quando al di fuori degli atti giudiziari parliamo di politici corrotti o collusi con altri poteri criminali, possiamo farlo a seguito di sentenze di condanna o di episodi inconfutabili e ormai pubblici (si pensi all'arresto in flagranza di un politico che riceva una mazzetta dal corruttore o ad una conversazione registrata ed ormai pubblica perché depositata in un processo). Anche in questo caso, però, bisogna farlo con sobrietà e misura, evitando improprie generalizzazioni di sapore qualunquistico (del tipo "i politici sono corrotti"), così evitando di offrire spunti per affermazioni altrettanto generalizzanti, quelle ben note e frequenti secondo cui l'esercizio obbligatorio dell'azione penale sarebbe in realtà conseguenza degli orientamenti politici dei magistrati. In un caso e nell'altro sono la democrazia e le sue istituzioni che perdono credibilità.

Si è già detto che protagonisti necessari della comunicazione relativa alla giustizia non sono solo i magistrati ma anche la polizia giudiziaria (se ne è già parlato nel par. 3), gli avvocati, i politici ed i giornalisti. Quest'intervento non è specificatamente dedicato anche a queste categorie, ma – avviandomi alla conclusione – qualche osservazione in merito è necessaria.

8. Avvocati e informazione

Ricordo quando Virginio Rognoni (sì, ancora lui), da ex vicepresidente del CSM, ebbe a definire virtuoso il protagonismo dei magistrati e degli avvocati civilmente impegnati a fornire corrette informazioni ai cittadini nell'interesse della amministrazione della giustizia e della sua credibilità.

Ma, così come è stato sin qui fatto per le criticità comunicative dei magistrati, non si può tacere in ordine a certi comportamenti di non pochi avvocati che sfruttano la risonanza mediatica delle inchieste in cui sono coinvolti i loro assistiti, ed anzi le amplificano.

Anche grazie a tale propensione si afferma il processo mediatico, che – maggiormente deprimente se vi partecipano magistrati – diventa spesso più importante ed efficace di quello che si celebra nelle Aule di Giustizia e della sentenza cui è finalizzato. Senonchè, come ha scritto Luigi Ferrarella[8], "su questo piano nessuno si salva, perché nel processo mediatico vince comunque il più scorretto, a prescindere dal lavoro che fa. Vince il magistrato più ambizioso o più vanitoso, come viene lamentato spesso; ma vince anche l'avvocato più aggressivo e scorretto; vince l'imputato (se mi si concede l'errore) più "eccellente", vince il poliziotto-carabiniere-finanziere meglio introdotto nel circuito mediatico ai fini della sua progressione in carriera o della sua logica di cordata interna; e vince il giornalista più spregiudicato. Con un risultato micidiale anche sul modo in cui in una collettività democratica viene amministrata la giustizia".

Ed a ciò deve anche aggiungersi che il consenso popolare viene televisivamente ricercato da qualche avvocato anche quale mezzo di proliferazione della propria clientela.

Inesistente, o comunque rara, è peraltro qualsiasi forma di autocritica della categoria anche rispetto a quegli avvocati che, subito dopo la pronuncia di una sentenza di condanna dei loro assistiti, anziché formulare, come è ben possibile, legittime critiche in modo pacato ed eticamente consentito, si lasciano andare a commenti delegittimanti nei confronti dei giudici che hanno emesso la sentenza.

Senza questo tipo di atteggiamenti i talk-show non avrebbero seguito e le telecamere non avrebbero ragione di popolare le aule di giustizia.

9. I politici che strumentalizzano l'informazione sulla giustizia

Non intendo qui far riferimento alle conosciute modalità di reazione a processi, condanne e assoluzioni da parte di politici a vario titolo incriminati. Il tema mi interessa poco anche perché è ovviamente prevedibile che un imputato, a qualsiasi categoria appartenente, ben difficilmente potrà essere riconoscente nei confronti di quanti lo hanno incriminato e condannato.

Mi interessa invece qualche breve cenno al comportamento di quei politici, con incarichi governativi o meno, che sono ben attenti a sfruttare le nuove moda-

[8] L. Ferrarella: "Proposta minoritaria di ecologia giornalistica" (2007).

lità di comunicazione che i tempi moderni hanno imposto: come si dirà appresso, si moltiplicano giornalisti inclini non tanto all'approfondimento della notizia dai politici propalata con insopportabile retorica, ma a determinarne comunque il massimo clamore.

Basti pensare a come, per mero scopo di supporto alle proprie scelte e posizioni, esponenti di rilievo di vari Governi (caratterizzati da diversa composizione politica) hanno presentato ai cittadini, da un lato, i famosi "pacchetti sicurezza" del 2008 e del 2009, e dall'altro, esattamente a dieci anni di distanza, gli altrettanto propagandati "decreti sicurezza" del 2018 e del 2019. Nel primo caso sono stati diffusi infondati allarmi sui rischi derivanti per l'Italia dal terrorismo internazionale (notizie riguardanti inesistenti scuole di kamikaze; inesistenti progetti di attentati a seggi elettorali, alla cattedrale di Bologna, alle stazioni metropolitane; o, ancora, la massiccia presenza dell'IS a Roma, i numeri esagerati di foreign fighters espulsi, la balla del marocchino arrestato in provincia di Milano – e poi scarcerato dai Giudici – perché complice dell'attentato al Bardo di Tunisi); nel secondo caso sono state ipotizzate inesistenti presenze di terroristi tra quanti arrivano in Italia sui barconi e calunniate le ONG titolari delle navi che effettuavano salvataggi in mare, accusate di collusioni con trafficanti di esseri umani. In entrambi i casi, va ricordata la evidente propalazione di pulsioni xenofobe nei confronti degli immigrati, descritti come veri e propri nemici da non far entrare in Italia e/o da rispedire il più velocemente possibile negli Stati d'origine, ignorando le drammatiche situazioni ivi esistenti ed i cogenti principi, di livello costituzionale ed internazionale, in tema di asilo politico, protezione internazionale e tutela dei diritti fondamentali delle persone.

Insomma la notizia che dovrebbe servire ad informare correttamente serve in realtà, come nei casi appena citati, ad enfatizzare il problema sicurezza, così da allarmare i cittadini ed insieme rassicurarli grazie a continui riferimenti alla capacità di chi governa di saperli tutelare attraverso apparati di intelligence e leggi sapienti. Zygmunt Bauman ci aveva già avvertito in odine al senso di questa strategia politica che serve a far passare in second'ordine – rispetto all'abusato tema della sicurezza – problemi sociali ed economici, doveri costituzionali ed incapacità di guida politica del paese. E per tutto questo, ora, basta un tweet o un sms di 160 caratteri: forse lo stesso Bauman non l'aveva immaginato!

10. I giornalisti che producono l'informazione sulla giustizia

I giornalisti, ovviamente, dovrebbero essere gli osservanti più scrupolosi delle regole della corretta informazione. E fortunatamente molti lo sono. Ma anche per questa categoria, la modernità ha imposto "anti-regole" pericolose ed inaccettabili.

Cito un altro episodio personalmente vissuto più di vent'anni fa allorchè, nel corso di un lungo viaggio di studio negli Stati Uniti, mi trovai a discutere, a Chicago, con il locale Prosecutor federale, in ordine al livello di indipendenza possibile dei Procuratori designati dal Presidente degli Stati Uniti (nel sistema di giustizia federale) o eletti (nel sistema di giustizia statale). Gli chiesi se i pubblici ministeri non fossero condizionati dalla fonte politica della loro nomina. La risposta fu "Caro collega, qui c'è la stampa!". Non disse "..la stampa libera". Alludeva al ruolo di cane da guardia del giornalismo d'inchiesta, forse troppo citato, ma che, come è noto, ha consentito – negli Stati Uniti – di far venire alla luce scandali di portata storica.

Il giornalismo d'inchiesta, in sostanza, negli Stati Uniti e dovunque, grazie ad approfondimenti seri, documentati e soprattutto liberi, dovrebbe ricercare la verità dei fatti, come spetta al PM nelle sue indagini giudiziarie.

È così anche in Italia? Purtroppo non è sempre così. Ho prima citato, a proposito dei politici, i vizi originati della moderna informazione, in modo particolare di quella ormai dominante (o quasi) sul web, che impone assoluta rapidità di diffusione delle notizie. Ma se ciò avviene senza approfondimenti e senza le dovute precisazioni, non è affatto una buona informazione, specie ove si pensi che, nei frequenti casi di diffusione via web di informazioni imprecise e superficiali, è molto difficile che l'indomani, i quotidiani titolari del siti web possano correggere ed ammettere l'errore.

Si sono però diffuse altre modalità poco corrette di interlocuzione ed informazione nel settore della giustizia (al quale mi limito): una parola di saluto e commento informale di un magistrato diventa intervista mai rilasciata o autorizzata, titoli in rilievo e virgolettati lasciano pensare a contenuti degli articoli ad essi conformi ed a dichiarazioni rilasciate da persona intervistata, mentre quasi mai quelle parole sono state pronunciate da alcuno e spesso i contenuti degli articoli ne smentiscono i titoli.

Parlandone con qualche autorevole giornalista amico, mi è stato risposto che quella è ormai la moderna tecnica utilizzata dai giornali per attirare l'attenzione del lettore.

E c'è molto altro: presenza di telecamere non autorizzate nei palazzi di giustizia, i cui utilizzatori sono pronti a riprendere persone che si recano negli uffici dei magistrati per essere esaminati o interrogati, con conseguente violazione della *privacy*; giornalisti che, come si è detto, pretendono di dar vita a rapporti confidenziali con i magistrati per avere accesso prioritario a notizie riservate o che nelle interviste pongono domande dai toni e contenuti provocatori per generare imbarazzo negli intervistati e perché ne resti traccia nei servizi televisivi; articoli che tendono ad assecondare le peggiori pulsioni populiste dei lettori etc.. Sono questi i principali vizi del giornalismo moderno che si occupa della giusti-

zia, fermo restando che non intendo spendere una sola parola sui professionisti disonesti. Ce ne sono infatti anche tra magistrati ed avvocati e non vi è necessità di alcun commento in proposito. Onore, invece, ai tanti giornalisti che fanno il loro dovere con assoluta professionalità e correttezza, senza sconti per alcuno. Ed onore a coloro che, in ogni parte del mondo, sono morti o sono stati perseguitati nell'adempimento del loro dovere.

Il mio sogno è di vedere il nostro mondo della giustizia popolato da giornalisti *"factcheckers"* che peraltro, anziché cercare documenti in modo scorretto, provvedano ad eventualmente richiederli con formali istanze (come da prassi introdotta a Torino[9]) ai sensi dell'art. 116 c.p.p.. Meglio ancora sarebbe, come da anni proposto da Luigi Ferrarella, disciplinare legislativamente il loro accesso agli atti, per evitare dipendenza da fonti portatrici di interesse e per esaltare la libertà e professionalità dei giornalisti.

11. La necessità di una riflessione comune su informazione e giustizia tra magistrati, avvocati e giornalisti

Al di là delle già citate regole disciplinari, sono da tempo intervenuti codici deontologici per magistrati[10], avvocati e giornalisti, cioè per tre delle principali categorie protagoniste del rapporto tra comunicazione e giustizia: tali codici sono sempre più mirati a disciplinare diritti e doveri connessi all'esercizio delle rispettive citate funzioni, ma i vizi sin qui esposti – ed altri ancora – permangono ed anzi rischiano di amplificarsi.

Non occorre – allora – invocare nuove regole deontologiche e sanzioni, quanto un confronto diffuso, serrato e sincero tra le categorie interessate a dar luogo a prassi corrette. Citando ancora una volta la mia esperienza professionale, devo dire che sono stati organizzati dalla Procura della Repubblica di Torino, tra il 2017 ed il 2018, vari incontri con i giornalisti ed un'assemblea anche con gli avvocati per discutere dell'irrinunciabile importanza della informazione sulla giustizia e dei connessi diritti – doveri, di cui, però, vanno anche conosciuti i confini,

---

[9] Si rimanda, anche in questo caso, a quanto si dirà più avanti in ordine ai Criteri di organizzazione della Procura della Repubblica di Torino, varati dallo scrivente l'8.10.2018, ed al relativo allegato.

[10] Per quanto riguarda i magistrati, l'art. 6 del Codice etico dell'ANM prevede quanto segue:
Art. 6 – Rapporti con la stampa e con gli altri mezzi di comunicazione di massa
Nei contatti con la stampa e con gli altri mezzi di comunicazione il magistrato non sollecita la pubblicità di notizie attinenti alla propria attività di ufficio ...omissis….
Fermo il principio di piena libertà di manifestazione del pensiero, il magistrato si ispira a criteri di equilibrio, dignità e misura nel rilasciare dichiarazioni ed interviste ai giornali e agli altri mezzi di comunicazione di massa, così come in ogni scritto e in ogni dichiarazione destinati alla diffusione.

diversi a seconda delle fasi del processo e comunque giustamente condizionati dal rispetto delle regole poste a tutela della *privacy* delle persone.

L'auspicio è che tutti i magistrati, qualunque sia la funzione da loro svolta (ma in particolare i pubblici ministeri, categoria cui ha appartenuto chi scrive per tutta la sua carriera), siano ben consapevoli che la propria autorevolezza e credibilità non dipendono dallo spazio e dal rilievo eventualmente riservati dalla informazione alla loro attività professionale, ai loro volti ed ai loro nomi, ma dai risultati attestati nelle sentenze definitive. È anche questo che dà corpo alla fiducia nella Giustizia.

Il magistrato, dunque, sia protagonista virtuoso di corretta comunicazione e di ogni utile interlocuzione nel dibattito sui temi della giustizia! Ma sia capace di esserlo con misura, anche in questo difficile contesto storico in cui qualsiasi intervento tecnico, persino in ordine ad un disegno di legge o in tema di diritti fondamentali, genera in automatico sempre la stessa strumentale risposta: "il magistrato taccia o scenda in politica", come se a tale tipo di interlocuzione fossero abilitati solo i politici mentre per i magistrati si tratterebbe di un'esondazione al di fuori dei confini del proprio doveroso agire! Deve essere ben chiaro, allora, che dipenderà soprattutto da noi (mi permetto di usare ancora la prima persona plurale, anche se ho lasciato la magistratura per raggiunti limiti di età) se i cittadini comprenderanno quali sono le ragioni per cui nessuno può farci tacere.

Note introduttive sull'Allegato che segue

Criteri di organizzazione della Procura della Repubblica di Torino, varati dal Procuratore della Repubblica *pro tempore* l'8.10.2018: parti concernenti le direttive in tema di rapporti dei magistrati e della polizia giudiziaria con gli organi di informazione

Le osservazioni fin qui formulate non devono essere considerate meramente discorsive e volte a stimolare solo dibattito teorico e dialettica sul tema in intestazione.

Chi scrive, infatti, ritiene che possano costituire la base di precise direttive nella formulazione di circolari e criteri organizzativi degli Uffici Giudiziari di competenza dei rispettivi dirigenti (in particolare dei Procuratori della Repubblica presso i Tribunali).

Per tale ragione, nella consapevolezza della delicatezza della materia e solo per contribuire a possibili riflessioni nell'ambito del Corso di formazione richiamato in prima pagina, lo scrivente ritiene utile allegare alla presente relazione le parti dei Criteri di organizzazione della Procura della Repubblica di Torino (che ha varato l'8 ottobre 2018 e che, composto da 242 pagine e 25 allegati, è consultabile sulla homepage del sito web dell'ufficio: *www.procura.torino.it*) concernenti le direttive in tema di rapporti dei magistrati e della polizia giudiziaria con gli organi di informazione.

Si rimanda, dunque, alle pagine seguenti.

ALLEGATO

Procura della Repubblica presso il Tribunale di Torino

(Prot. n. 3879/18 S.P.)

Criteri di organizzazione dell'Ufficio

per il periodo 8 ottobre 2018 – 31 dicembre 2019

(Torino, 8 ottobre 2018)

---===oOo===---

(sostituiscono le "Linee Guida" del 23.6.2015)

Pag. 221 dei Criteri Organizzativi:

21: Direttive per i magistrati dell'Ufficio, con particolare riferimento ai rapporti con la Polizia Giudiziaria

Sempre per quanto riguarda la direzione delle indagini, i Pubblici ministeri dovranno raccomandare alla polizia giudiziaria, ogniqualvolta ciò risulti utile o necessario, quanto segue:

…omissis…

22: evitare, specie in caso di indagini delicate, conferenze e comunicati stampa relativi ad attività di polizia giudiziaria, senza previo assenso del magistrato che le coordina.

…omissis…

---===oOo===---

Pag. 237 dei Criteri Organizzativi:

23: Rapporti con gli organi di informazione

La necessità ed il dovere di corretta informazione sulle attività connesse all'amministrazione della Giustizia, anche in relazione alla fase delle indagini preliminari quando le circostanze lo consentano e comunque mai in violazione del segreto e delle previsioni di cui all'art. 2, comma 1, lett. "u", "v" ed "aa" del D.lvo 23 febbraio 2006 n. 109 (*Disciplina degli illeciti disciplinari dei magistrati, delle relative sanzioni e della procedura per la loro applicabilità*…[1]), come

[1] Queste le previsioni di cui alle lettere "u", "v" ed "aa" dell' art. 2, comma 1 del D.L.vo 109/2006:
1.1. Costituiscono illeciti disciplinari nell'esercizio delle funzioni:
u) *la divulgazione, anche dipendente da negligenza, di atti del procedimento coperti dal segreto o di cui sia previsto il divieto di pubblicazione, nonché la violazione del dovere di riservatezza sugli affari in corso di trattazione, o sugli affari definiti, quando è idonea a ledere indebitamente diritti altrui;*
v) *pubbliche dichiarazioni o interviste che riguardino i soggetti coinvolti negli affari in corso di trattazione, ovvero trattati e non definiti con provvedimento non soggetto a impugnazione ordinaria, quando sono dirette a ledere indebitamente diritti altrui nonché la violazione del divieto di cui all'articolo 5, comma 2, del decreto legislativo 20 febbraio 2006, n. 106 (2)*;

modificato con Legge 24 ottobre 2006, n. 269, appaiono evidenti anche al fine di evitare sviamenti e strumentali rappresentazioni della verità dei fatti.

In ossequio al disposto dell'art. 5 del d.L.vo 106/2006 ed anticipando il contenuto della delibera adottata dal C.S.M. nella seduta dell'11 luglio 2018 (prot. num. 310/VV/2017 – Linee-guida per l'organizzazione degli Uffici giudiziari ai fini di una corretta comunicazione istituzionale), lo scrivente aveva già dettato, in occasione della emanazione dei Criteri organizzativi del 23 giugno 2015, precise direttive che appresso si richiamano e si confermano, nell'ottica del rispetto dei doveri nei confronti degli individui (rispetto della vita privata e familiare, della sicurezza e della dignità) e dei doveri di matrice processuale (rispetto del giusto processo e dei diritti della difesa, con tutela della presunzione di non colpevolezza che la Corte Edu raccomanda anche con riferimento alle parole da usare nell'informazione; rispetto della centralità del giudicato, dei diritti delle vittime dei reati, del diritto di indagati ed imputati di non apprendere dalla stampa quanto gli dovrebbe prima essere comunicato formalmente; il dovere del P.M. di rispettare le decisioni giudiziarie contestandole solo nelle sedi processuali proprie e, in particolare, con le eventuali impugnazioni).

I rapporti con gli organi di informazione saranno tenuti direttamente dal Procuratore della Repubblica o dai Coordinatori dei vari gruppi da lui delegati (in base anche alla circolare del CSM relativa all'applicazione del citato art. 5).

Tale principio è stato dal sottoscritto ribadito, sin dall'assunzione delle proprie funzioni, a tutti i Sostituti, a cui è stato fatto divieto, salvo eccezioni espressamente autorizzate dal Procuratore, di partecipare a conferenze stampa o di emettere comunicati stampa o di fornire comunque agli organi di informazioni notizie concernenti l'attività giudiziaria dell'ufficio.

Le comunicazioni in ordine alle attività della Procura, che saranno ritenute utili e compatibili con le esigenze di segretezza delle indagini e che comunque verranno diffuse attribuendo le attività in modo impersonale all'ufficio ed escludendo ogni riferimento ai magistrati assegnatari dei procedimenti (art. 5 co. 2 D. L.vo 160/2006), verranno pertanto effettuate, normalmente a mezzo di comunicati stampa, dal Procuratore della Repubblica (quale *responsabile per la comunicazione*) d'intesa con il Coordinatore del gruppo specializzato (o dal Coordinatore stesso, in assenza del Procuratore) competente in ordine alle attività d'interesse, nelle forme e con i tempi che saranno valutati opportuni.

---

aa) *il sollecitare la pubblicità di notizie attinenti alla propria attività di ufficio ovvero il costituire e l'utilizzare canali informativi personali riservati o privilegiati*;

Attraverso i comunicati stampa, potranno essere garantite precisione e sinteticità della informazione, inoppugnabilità del testo diffuso che risultano particolarmente necessarie in un contesto informativo che, spesso scorrettamente, determina la pubblicazione virgolettata di affermazioni mai rilasciate o sintesi strumentalmente imprecise, il tutto nell'ottica di attirare l'attenzione del lettore disinformato.

Solo eccezionalmente il Procuratore disporrà la diffusione pubblica di notizie attraverso conferenze stampa, scelta che motiverà nelle rispettive occasioni.[2] A tali conferenze stampa potranno partecipare i magistrati interessati, designati dal Procuratore della Repubblica.

I sostituti segnaleranno ai Coordinatori dei Gruppi specializzati cui appartengono (o direttamente al Procuratore) le occasioni in cui ritengano utile la diffusione di comunicati stampa relativi alle indagini da loro dirette o l'eventuale organizzazione di una conferenza stampa, assemblando e controllando le informazioni da rendere pubbliche.

Naturalmente, nei rapporti con la stampa, questo ufficio curerà, oltre il rispetto dei principi già citati:

- la non interferenza delle informazioni con indagini ed esercizio dell'azione penale, né con eventuali segreti investigativi né con doveri ed esigenze di riservatezza che ne possano risultare compromessi;
- l'osservanza del divieto di diffusione di fotografie ed immagine di persone in manette;
- l'osservanza del divieto di diffusione di immagini e generalità dei minori;
- reciproco rispetto e parità di trattamento rispetto a tutti gli organi di informazione, evitando ogni impropria rappresentazione dei meriti dell'azione dell'ufficio o dei servizi di polizia giudiziaria;

---

[2] Può essere utile ricordare che, da quando ha assunto l'attuale funzione dirigenziale, cioè dal 30.6.2014, lo scrivente ha tenuto solo quattro conferenze stampa: la prima per denunciare pubblicamente, insieme ai Presidenti del locale Consiglio dell'Ordine degli Avvocati e della Camera Penale, il grave deficit di personale amministrativo dell'Ufficio; la seconda su richiesta di altra A.G. di paese straniero per un'indagine di rilievo internazionale; la terza per illustrare i risultati ostensibili delle indagini sui gravi fatti verificatisi in Torino, in Piazza San Carlo, il 3 giugno 2017 e l'ultima per presentare pubblicamente le direttive emesse il 9 luglio 2018 in tema di priorità da accordare alla trattazione dei reati connotati da odio razziale ed al fine di velocizzare le procedure relative ai ricorsi avverso il rigetto delle richieste di protezione internazionale. Tali comunicazioni si pongono in linea con quanto previsto dalla citata delibera del CSM dell'11 luglio 2018 che prevede che il Procuratore della Repubblica "*..assicura l'informazione sull'organizzazione e sull'attività della procura nel quadro della generale esigenza di trasparenza dell'organizzazione giudiziaria*.".

- la necessità che anche gli organi di polizia giudiziaria osservino i criteri sin qui elencati;
- il divieto di utilizzo negli uffici della Procura di telecamere ed apparati fotografici, senza specifica autorizzazione.

Ai Sostituti, naturalmente, è fatto obbligo di massimo riserbo (con connesso divieto di rilasciare dichiarazioni) anche in ordine all'attività giudiziaria di altri magistrati dell'ufficio.

Il Procuratore, come è tenuto a fare e come precisato anche nei criteri organizzativi del giugno 2015, vigilerà anche su possibili violazioni disciplinari concernenti le violazioni del dovere di riservatezza, competendogli l'obbligo di segnalare al Consiglio Giudiziario, per l'esercizio del potere di vigilanza e di sollecitazione dell'azione disciplinare, le condotte dei magistrati dell'ufficio che siano in contrasto con le predette disposizioni (art. 5 co. 4 D. L.vo 160/2006).

Va anche ricordato che, con comunicazione del 15 ottobre 2015 (Prot.n. 84/15 Int.) sui *Rapporti con i mezzi di informazione* (integranti le disposizioni già contenute nei criteri di organizzazione dell'Ufficio del 23.6.2015), lo scrivente ha raccomandato ai magistrati dell'Ufficio, a seguito di criticità manifestatesi, non solo il rispetto delle predette direttive, ma anche un efficace controllo sulle comunicazioni provenienti da Comandi ed uffici di Polizia Giudiziaria.

A tale ultimo proposito deve essere qui confermata la prassi concordata con i vertici dei presidi di Polizia Giudiziaria operanti nel Circondario secondo la quale, anche in occasione di comunicati stampa da essi predisposti, la relativa bozza dovrà tendenzialmente essere sottoposta all'esame della Procura della Repubblica prima della diffusione.

Sempre in linea con quanto previsto dalla citata delibera del CSM dell'11 luglio 2018, che prevede che il Procuratore della Repubblica "*..assicura l'informazione sull'organizzazione e sull'attività della procura nel quadro della generale esigenza di trasparenza dell'organizzazione giudiziaria.*", il Procuratore curerà, con l'ausilio dell'Ufficio Informatico, il costante aggiornamento del sito internet dell'Ufficio.

Infine, poiché, al di là delle parti processuali, spesso avviene che giornalisti, associazioni ed enti vari, privati a vario titolo interessati chiedano il rilascio di copie di atti processuali di procedimenti in corso di trattazione dibattimentale o già da tempo definiti, si raccomanda a tutti i magistrati dell'Ufficio l'attento rispetto di quanto previsto dall'art. 116 c.p.p. in ordine alla valutazione sia dell'interesse del richiedente, sia della competenza a provvedere sull'istanza (ove tale

competenza sia del giudice che procede al momento della presentazione della domanda o del presidente del collegio o del giudice che ha emesso provvedimento di archiviazione o sentenza, il pubblico ministero formulerà comunque il suo parere).

---===oOo===---

Dispositivo finale: pag. 241 dei Criteri Organizzativi

Pertanto,

IL PROCURATORE DELLA REPUBBLICA

DISPONE

quanto segue

L'emanazione dei presenti Criteri Organizzativi della Procura della Repubblica presso il Tribunale di Torino, con conseguenti modifiche a quelli del 23.6.2015.

Il presente provvedimento avrà efficacia a partire dalla data odierna.

Per quanto in esso non previsto, si rimanda (anche per le specifiche procedure da rispettare) alla Circolare del CSM del 16.11.2017 sull'Organizzazione degli Uffici di Procura

Più in generale, alla luce della qualità e quantità degli interventi innovativi derivanti dai presenti Criteri organizzativi della Procura della Repubblica di Torino, il Procuratore si riserva, dopo necessaria e periodica valutazione dei conseguenti effetti, di apportarvi i correttivi che si rendessero eventualmente necessari.

Dispone altresì

la trasmissione del presente provvedimento ai diretti destinatari in servizio presso questa Procura della Repubblica, cioè a tutti i magistrati, a tutti i Vice Procuratori Onorari, alla Dirigente Amministrativa ed a tutto il personale amministrativo, nonchè ai responsabili delle Aliquote della Sezione di P.G. (che ne cureranno la diffusione anche per il personale di P.G. qui aggregato);

nonché, con supporto informatico in allegato, per quanto di rispettiva competenza e comunque per conoscenza:

– al Consiglio Superiore della Magistratura, a norma dell'art. 1 co. 7 D.lgs n. 106/2006, come modificato dalla l. 269/2006:
– al Consiglio Giudiziario presso la Corte d'Appello di Torino;
– al Procuratore Generale presso la Corte di Cassazione ed al Procuratore Nazionale Antimafia ed Antiterrorismo;
– al Presidente della Corte d'Appello ed al Procuratore Generale della Repubblica presso la Corte d'Appello di Torino (in questo caso, anche con riferimento alla circolare del 31 luglio 2017 – prot. 5964/pers./2018, con la quale il Procuratore Generale di Torino ha richiesto che gli siano trasmesse, con tempestivi aggiornamenti, le comunicazioni relative ad assegnazioni, trasferimenti, pensionamenti e dimissioni del personale di polizia giudiziaria, nonché relative ad applicazioni, aggregazioni e distacchi presso le Sezioni di P.G. delle Procure del Distretto);
– al Presidente del Tribunale;
– al Presidente del Consiglio dell'Ordine degli Avvocati di Torino;
– al Presidente della Camera Penale "V. Chiusano" di Torino;

Dispone che, a cura dell'Ufficio Informatico, i presenti Criteri Organizzativi, unitamente a tutti gli allegati vengano inseriti e resi accessibili nel sito web della Procura della Repubblica di Torino,

Torino, 8 ottobre 2018

IL PROCURATORE DELLA REPUBBLICA
Armando SPATARO

Finito di stampare nel mese di dicembre 2021
a cura di

POLIGRAFICO
E ZECCA
DELLO STATO
ITALIANO
IPZS S.p.A.


POLIGRAFICO
E ZECCA
DELLO STATO
ITALIANO